How to Avoid Electronic Eavesdropping & Privacy Invasion

HOW TO AVOID ELECTRONIC EAVESDROPPING and PRIVACY INVASION

by William W. Turner

TABLE OF CONTENTS

Prologue

PART I

ORIGINS OF THE SPY STATE 5
Testimony of a Debugging Expert; the "Right to Privacy"; Bugging in Nazi Germany and Russia; Bugging by U.S. Government Agencies; Testimony of a Plain Clothesman; The "Black Bag Job"; FBI Bugging in Las Vegas; Where the Bugging Technicians Learn Their Trade; Bugging Devices Available to the General Public.

THE TELEPHONE TAP 7
How the Telephone System is Vulnerable to Taps; Inductive Taps; Metallic Taps; Cooperation of Telephone Companies with Snoopers; Checking for a Phone Tap; If a Phone Tap is Discovered . . . ; Preventative Measures.

WIRED MIKES AND BUGGED TELEPHONES 44
Advantages of Using Wired Mikes; Installation Techniques; Different Types of Wired Mikes; Using the Telephone as a Wired Mike; Checking for Wired Mikes; Preventative Measures.

THE WIRELESS BUG 56
Advantages and Disadvantages of the Wireless Bug; The Voice Operated Relay; Wireless Bugs in the Telephone; Models and Prices of Wireless Bugs; Checking for Bugs; Using the TV Set as a Bug Detector; Preventative Measures.

THE ROOM NEXT DOOR 78
The Spike Mike; The Contact Mike; The Stethoscope Mike; The Shotgun Mike; The Parabolic Mike; Preventative Measures.

THE BUMPER BEEPER 86
An Elementary Automobile Tailing Device; How Bumper Beepers Operate; Detecting the Presence of a Bumper Beeper; Preventing Bumper Beepers Being Attached to Your Car.

PART II

INDUSTRIAL ESPIONAGE 93
The Magnitude of Industrial Espionage; Firms Who Specialize in Bugging Protection for Industry; How the Industrial Spy Operates; Actual Reports of an Operative spying on a large New England Drug Company; Maintaining Security and Employee Loyalty; The Trash Cover.

PART III

THE LAW 151
Only Government Agencies Can Bug Legally; Bugging Laws and the Police; Prosecutions for Illegal Bugging; Survey of Electronic Eavesdropping in the Omnibus Crime Control and Safe Streets Act of 1968.

REPRINT OF TITLE III: The Law Covering Wiretapping and Electronic Surveillance. 158

Epilogue 187

Appendix: Radio Bands and Their Uses 188

Glossary 189

Prologue

Nobody knows the extent of electronic eavesdropping in the United States, although all signs point to it being widespread and democratic in its choice of victims. If you happen to be married with a suspicious spouse, a manufacturer with proprietary secrets, a bidder on a large contract, a football coach, politician, policeman, insurance beneficiary, tax cheat, heroic guerrilla, blackmail prospect, gambler, union official, government employee, plaintiff in a law suit, lawyer on a big case, black or white militant, society doyen, hotel guest, or one of numerous other types, you may be the target of a sonic voyeur.

There is no cause for paranoia—although paranoia there is. But any individual or firm seeking to preserve his privacy, whether for personal reasons or monetary ones, is well advised to consider the possibility. The offices of many auto showrooms are bugged, so that the salesman can overhear the husband and wife conferring. Some motel rooms are bugged, so that the proprietor can detect extra nonpaying guests. A socially prominent couple hired private detectives to bug each other until the court ordered them to cease and desist.

In a number of cases corporate morality has been corrupted to the point of condoning eavesdropping to obtain vital information from competitors. This is not surprising, since the stakes run into the hundreds of thousands and occasionally millions of dollars. The more competitive the industry – ranking high are oil and gas, utilities, law, labor, chemicals, beer and liquor, cos-

metics, publishing — the better the chance that an eavesdropper is at work. The fact that in only a little more than 5 percent of the cases involving a complaint have devices been found is not altogether reassuring. When information leaks are suspected, the victim may attribute his loss to other causes such as dishonest employees and copied documents.

Says San Francisco private investigator Harold Lipset: "Bugging is less dangerous than betting, harder to prove, and more profitable." It is profitable for the eavesdropper as well as his client; prices range from $100 for a quick installation in a marital case to thousands of dollars in large industrial espionage situations.

If you suspect you may be tapped or bugged, there are steps you can take. By a few simple, preliminary steps, you can find inexpertly placed bugs. By calling the phone company, you can have a free check of your phone line (with strings attached, which we will deal with later). And if you can pay the price you can hire the services of an expert debugger. Then, too, there are precautionary moves that can prevent the placement of a bug or tap and, if one is already in, thwart the listener.

We will discuss all this in the following pages. But first, we should take a look at the current state of affairs.

PART I

ORIGINS OF THE SPY STATE

"It is a sad fact but true that most public officials and businessmen in America today are afraid to use the telephone except for the most casual conversations," commented Governor Grant Sawyer of Nevada in 1966 after 22 FBI bugs were ferreted out of Las Vegas casinos.

"I can't talk to you on the phone," San Francisco supervisor Roger Boas quoted Washington officials with whom he wanted to discuss city business. "The phone is probably tapped." When Boas showed up in their offices, they were still reluctant to talk openly, fearing bugs in the wall.

When the Washington *Post* did a survey of eavesdropping in the nations capital in February, 1971, it found that "about a quarter of the senators, congressmen, lawyers, businessmen and journalists . . . said they have suspected or believed that their telephones were tapped or their offices bugged."

An idea of the extent of industrial espionage may be gained from the following testimony from the government's Invasions of Privacy Hearings, conducted by Senator Long.

TESTIMONY OF ROBERT HUERTA, GLEN COVE, N.Y.

Senator Long. Mr. Kass, will you conduct the interrogation, please?

Mr. Kass. Thank you, Mr. Chairman.

Mr. Huerta, state your name and address, please.

Mr. Huerta. *I am Robert Huerta and I live at 2 Hemlock Lane, Glen Cove, N.Y.*

Mr. Kass. And your position?

Mr. Huerta. *I am a private investigator.*

Mr. Kass. Are you in the profession commonly known as debugging?

Mr. Huerta. *That is correct.*

Mr. Kass. Would you describe for the committee some of the activties you have done?

Mr. Huerta. *Yes; I have been engaged primarily in the debugging aspect for the past 2 or 3 years, since the average industry has been advised that there are devices around to intercept telephone calls and to intercept board meetings and such. So I have been detained by various companies, mainly manufacturing companies, oil companies, people in the cosmetics industry, stock brokers, law firms, and other people that are in big industry, to check to see if their telephones or their conference rooms are being bugged by people that have interests in their business and are looking to gain information by this particular bugging.*

Mr. Kass. Where do your checks primarily take place?

Mr. Huerta. *In the particular offices, in their board rooms, on their private telephones, in their homes, and also if they are utilizing hotel rooms for conferences, we would check these rooms out prior to their meetings.*

Mr. Kass. Do you keep a continuous surveillance on a board room while a meeting is going on?

Mr. Huerta. *Sometimes yes, sometimes no. Sometimes we make a check prior to the meeting. We hope that the individuals that are coming into the meeting, of course, are not carrying concealed tape recorders or units on them. Sometimes we monitor the entire meeting to see if there are any transmitters being used during this particular meeting.*

Mr. Kass. You stated you worked for various industries. Could you capsulize, without mentioning the names of the companies, the type of industries you work for?

Mr. Huerta. *Well, major oil companies, major pharmaceutical companies, large manufacturing companies, people in the liquor industry, the soft drink industry. I guess just about every type of major industry that is around in New York and other States also. Plus individuals, law firms, and private persons, the film industry, Hollywood stars, you might say.*

Mr. Kass. Domestic-type situations?

Mr. Huerta. *Domestic-type situations; yes.*

Mr. Kass. Any political-type situations?

Mr. Huerta. *Yes.*

Mr. Kass. Mr. Huerta, you said the liquor industry. Were you involved in the Rosensteil episode? The subcommittee took testimony a year ago that a bug was found in Mr. Rosensteil's room.

Mr. Huerta. *Yes, I was.*

In fact, I found a bug in Mr. Rosensteil's private home in Florida and I also found a drop off his private line down in Miami, Fla.

Mr. Kass. Was there any evidence that there

was some wiretapping involved in that?

Mr. Huerta. *Definitely.*

Mr. Kass. You said you have done some work for various industries. Have you found any bugs?

Mr. Huerta. *Yes; I have found not only bugs. I found transmitters, you might say, that have been expended and used. People have called us in after the desired information has been out. We have found transmitters. Of course, they are all battery operated and they have been expended for some time. We can't really tell.*

We have also found evidence of wiretaps on individuals that we have not been able to tie down to any particular person, but there are occasions when we have found evidence of wiretapping.

Mr. Kass. What happens when you find a bug for a company? What is the next step?

Mr. Huerta. *Some companies will like to find out who is the culprit. We institute an investigation to try to ascertain who placed the bug or for what purpose it was placed. Other companies are really reluctant to do anything about it for fear of publicity. They would rather not have their names mentioned in connection with bugging or anything else so they would just as soon keep this more or less under the table.*

Mr. Kass. How much do you get paid for an average debugging job?

Mr. Huerta. *For a particular telephone instrument like this in one office, if it is only one instrument, I would say approximately $75. If it is the entire room, it may run to $125.*

If it is a series of offices, it might run to $300, $400, $500, depending on the time it takes to do the job.

Mr. Kass. This includes your expenses and transportation?

Mr. Huerta. *They would, of course, pay any travel expenses. I fly around the country.*

Mr. Kass. You do fly around the country to do a job?

Mr. Huerta. *Yes, I do.*

Mr. Kass. Mr. Huerta, if you were given a job to bug an office or put a tap on a phone, how would you enter an apartment or an office building.

Mr. Huerta. *Well, there are various ways. From my experience in finding the various bugs that have been installed, I feel that most persons are very lax in their security. I think as far as the company goes, the easiest way would be to become a cleaning man, we will say, find a cleaning company that cleans the various premises and he would just take a job up with these people. When it came to your turn to clean that particular floor or that particular office, you would just install the bug or the telephone tap, whichever is desired.*

Mr. Kass. Is it an easy job to become a cleaning man?

Mr. Huerta. *Certainly; there are cleaning companies in New York looking for able-bodied young men, we might say, to push a broom and swing a mop. You can desire — well, you can say, "I am an oddball and I would like to clean 500 Fifth Avenue. I like the building,*

I like the environment"; and they will hire you because they need the people.

Mr. Kass. Aren't they wise to these things?

Mr. Huerta. *Not necessarily.*

Mr. Kass. Are they in cahoots with them?

Mr. Huerta. *I think certain people may pay $5 or $10 to gain a job or maybe more than that. But, on the average, they just don't question a person's desire to work in a place.*

Mr. Kass. In other words, they don't care?

Mr. Huerta. *They just don't care. They need the people. And they hire them.*

Mr. Kass. So the person does some extra bugging on the side, and the company doesn't seem to mind; is that right?

Mr. Huerta. *Exactly.*

Mr. Kass. You say there are various ways of entering. What are other ways besides a cleaning establishment?

Mr. Huerta. *In other words, if you have a particular floor you are interested in, you might hang around that floor about 5 o'clock and hide in the men's room, or after a particular individual has left a busy desk, you might sit there and assume the role of the busy, up-and-coming executive and sit at a desk until everybody has left and have the room to yourself.*

Mr. Kass. There is very little security, in your opinion, in some of these large office buildings?

Mr. Huerta. *Exactly. There is no security, you might say.*

Mr. Kass. Mr. Huerta, have you ever done any work in the Senate Office Building?

Mr. Huerta. *Yes, I have.*

Mr. Kass. Did you find anything?
Mr. Huerta. *No, I did not.*
Mr. Kass. No more questions, Mr. Chairman.

Senator Long. Any questions, Mr. Fensterwald?
Mr. Fensterwald. I have no questions.

Senator Long. Mr. Waters?
Mr. Waters. Mr. Huerta, it would appear from the line of work you are engaged in that there are a great many people who are concerned about the security of what they intend to be private conversations; is that right?
Mr. Huerta. *That is correct, sir.*
Mr. Waters. About how many people would you say do the type of work you do?
Mr. Huerta. *How many investigators?*
Mr. Waters. Yes.
Mr. Huerta. *I have no idea, sir. I would estimate that there are probably maybe 50 or 60 in the New York area that might be involved in it. There are a number of people that you might say are out to gain a dollar and are in the business and do not have the know-how. But there are a few that are really experienced in the business and know exactly what they are looking for and have the know-how.*
Mr. Waters. It would appear from the testimony you have given to the subcommittee that it does take a certain amount of expertise to develop the type of mechanisms that are concealed and capable of being concealed and camouflaged so that they won't be detected after they are actually installed; correct?

Mr. Huerta. *That is correct. The transmitters and bugs used today are quite sophisticated. They have a range, I would say, anything that you might have available on the market today which might transmit up to a mile and a quarter. These are small, compact, and they certainly serve the purpose.*

Mr. Waters. Are they available to anybody who might walk in off the street?

Mr. Huerta. *Absolutely. I have purchased these myself for test purposes and they are available to anybody. No questions asked.*

Senator Long. Do you do all your work in the defensive areas?

Mr. Huerta. *Yes, sir.*

Senator Long. You place no bugs yourself?

Mr. Huerta. *No sir; I do not.*

Senator Long. Have not?

Mr. Huerta. *No, sir?*

Mr. Fensterwald. Mr. Huerta, do you have any contact with answering services?

Mr. Huerta. *No; I do not, sir.*

Mr. Fensterwald. How about locksmiths?

Mr. Huerta. *Do I have personally? I know personally that locksmiths do become involved or are available to certain investigators who might require access to particular apartments or buildings. This is something that with the mastering device that is used for office buildings and also apartment buildings — to obtain, we will say, one lock cylinder from a large apartment building or a large office building, any qualified locksmith could take one cylinder and give you a master key which*

would open any room or any apartment in the building with no problem. He would just make the code down.

Mr. Fensterwald. That is the testimony we heard yesterday and we understand that there are private detectives here in Washington — I don't know about New York — that have master keys to the main hotels and office buildings in this city.

Mr. Huerta. *This could be, sir. Once you acquire a key, of course, most investigators are reluctant to part with it.*

Mr. Fensterwald. If you obtain the lock from any one office in that building, you can make a master key from it?

Mr. Huerta. *That is correct. And some office buildings have some master keys for particular floors, but any good locksmith, if you obtain one cylinder from a particular office, there is always one master key or grand master key, as they classify it, for the entire building, which a superintendent would have to have in the event of fire or break-in or something like that. So he would be qualified to cut a key which would be a grand master key for the entire building. Of course, the people in the know would be able to obtain this key and have access, during the weekend, you may say. You can sign the book for an elevator operator, sign John Jones, 14th floor and the operator is reluctant to question you because he might insult you, you might be a member of this very fashionable firm that you are going to bug or tap.*

Mr. Fensterwald. So it is not difficult to gain access to plant a bug or tap in an office build-

ing?

Mr. Huerta. *I would say no. There are some companies that have stringent security measures, but most companies do not.*

Mr. Fensterwald. I have nothing more.

Senator Long. Thank you, Mr. Huerta. We appreciate your help and the authority with which you speak. We pushed you perhaps a little more than we would have liked. You have been very helpful.

This commentary on the American electronic spy state is far from isolated. Surveillance by electronic device is but one phase of a massive invasion of the privacy of the individual citizen and his business, social, and political groups.

With the rapid growth of our population, the overall complexity of our society, and the often necessary dependence of individuals upon one another for service and support, there is an increasing need for people to live in the presence of others. Yet the fundamental human claim to personal freedom, privacy, and dignity remains with each of us. Privacy is the right to live one's life according to one's own life style, to maintain one's own intimate, personal and confidential affairs, and to express thoughts and share feelings without fear of being observed by unwanted persons outside one's own private and personal domain. In short, privacy is the right to be left alone.

Frequently this precious right is overridden not by legislation but by the "big ear" of the snooper. Although eavesdropping has always been an in-

tegral part of society, the methods in use today are highly sophisticated. Today the eavesdropper can be far removed – as far as three thousand miles – from his victim and yet hear every word. Such is the state of the technology.

Privacy is a legal right developed over the years in Western society. The basic concept of privacy as protection for the individual's dignity is covered in the First Amendment to the Constitution, which concerned itself with freedom of speech and the concomitant liberty of silence. The right of privacy is implicit in the Fourth Amendment's safeguard against unlawful search and in the Fifth Amendment's mandate for due process and privilege against self-incrimination. It is, in fact, embodied in the fundamental concept of the pursuit of life, liberty, and happiness.

In 1928 the venerable Supreme Court Justice Louis Brandeis said of privacy:

> *The Makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure, and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions, and their sensations. They conferred, as against the Government, the right to be left alone – the most comprehensive of rights and the right most valued by civilized men.*

History tells of one modern society that abandoned all forms of individual privacy, the Third

Reich. Under the guidance of Adolph Hitler, the total destruction of citizens' rights to privacy became a principal weapon in the Nazis' efforts to gain iron-clad control of the German people and their vanquished nations. Among the most successful of the methods employed by the Gestapo and its companion units to spy on the populace were wiretapping and electronic eavesdropping. Even in the 1930's the technical acumen of the Germans had placed them in the forefront in the development of snooping devices.

Russia under the Czars was hardly better. A book by its last chief, the late A. T. Vassilyev, *The Ochrana, The Russian Secret Police*, is revealing on this score. The Ochrana functioned before the days of electronic surveillance, but it was thorough in applying the methods available to it and ruthless in its justifications. Its agents were skilled in planting informers and intercepting private correspondence, including invisible inks and codes. The Czar was even supplied with copies of private letters in which the great Russian writer Tolstoy "had given expression to his anti-militarist views." Writing from exile in London, Vassilyev assured that the methods were "never directed against orderly subjects of the Czar but only seditious elements." The dread reputation of the Ochrana, he contended, was to be "ascribed to the propaganda" of revolutionaries.

Although the Soviet Union today seems to have rid itself of the worst evils of the Stalin era, it is still essentially a police state, as the ordeal of Russian writers bears witness. It is kept so by the activities of the KGB (commissariat of state security), a lineal descendent of the Ochrana.

The KGB, naturally, is well versed in the art of electronic snooping. But the Soviet Union is not the only superinquisitive state. For example, businessmen traveling to certain South American military dictatorships know that all telephone calls in and out of the countries are monitored by the government.

Although not yet of the same horrendous social implications that evolved from such tragedies as Nazi Germany, an awesome specter has risen over the United States today: the constant invasion of privacy through the use of eavesdropping equipment, some sophisticated, some comparatively crude. Documented cases, presumably the tip of the iceberg, have been sufficient in number to spread a growing fear among Americans that it could happen to them, whatever their secrets.

The 1971 disclosures of Army snooping on civilians, including Adlai Stevenson III, and the hearings of Senator Sam Irvin's subcommittee on privacy invasion did nothing to allay these fears. But at the vanguard of the electronic onslaught are law enforcement agencies, both at the federal, state, and local levels. Even as staunch an advocate of legalized wiretapping against organized crime as Deputy Director Henry Ruth of the National Crime Commission concedes that government eavesdropping has generated a widespread paranoia that no amount of reassurance can dispel.

Yet the public has acquired a strange ambivalence toward electronic snooping, possibly because the government has justified the use of totalitarian means to attain the lofty end of extinguishing organized crime and preserving "na-

tional security." A 1969 Gallup Poll showed that 46 percent were in favor of permitting the government to indulge in it, with 47 percent opposed and 7 percent undecided.

This ambivalence has marked the history of law enforcement wiretapping and bugging. In the landmark Olmstead case of 1928, the Supreme Court ruled that since wiretapping did not ordinarily involve physical trespass, it was not tantamount to unreasonable search and seizure in violation of the Fourth Amendment. However, in 1934, Congress passed the Communications Act, Section 605 of which forbade wiretapping. The intent was to dissuade telephone company employees who were taking advantage of their positions to assist private detectives in tapping. The act did not dissuade the government, however, even though it was not excepted by the law. As World War II loomed, President Franklin D. Roosevelt granted the FBI executive authority to tap in national defense matters. The authority was extended to criminal-type cases such as kidnapping and extortion in which a life might be in danger. Even when the war emergency ended, the tapping went on. The Department of Justice took the position that no succeeding President had countermanded Roosevelt's order and, besides, the Communications Act was not violated because intelligence data was not disclosed outside the department — disclosure being a necessary element.

The trouble was that the definition was unilateral as to what constituted "national security." Consequently we have seen such dangerous absurdities as Mrs. Eleanor Roosevelt being tapped by Army intelligence during World War

II, the Stevenson incident, and FBI electronic surveillances of Dr. Martin Luther King Jr. In 1966 self-avowed electronic snooping expert Bernard B. Spindel testified before a special Massachusetts legislative commission that many members of Congress were tapped and that it was possible to secretly monitor White House telephones. Although the Department of Justice denied the allegation, Spindel insisted that he knew of a special branch line leading from the main congressional circuits to a nearby building. "One of the tenants of the top floor of this building was a Justice Department agency," he said.

Although the FBI has been caught in the act most frequently, other federal agencies have been equally promiscuous in their tapping and bugging. Hearings held by the Senate Subcommittee on Administrative Practice and Procedure in the late 1960's revealed that the Internal Revenue Service, Post Office Inspection Division, Food and Drug Administration, Customs Agency Service, Bureau of Narcotics, Central Intelligence Agency, and the various military intelligence agencies carried on extensive electronic surveillance. The IRS, for instance, reportedly possessed $3-million worth of electronic equipment, with the aggregate for all federal agencies being in the $20-million bracket. This figure is exclusive of the CIA, which has sophisticated devices that attach to telephone trunk lines and automatically separate and record hundreds of conversations.

To further estimate the scope of electronic snooping, the activities of local police agencies must be taken into account. The police, too, felt that the Communications Act was not intended to hamper them. Some states, notably California,

forbade tapping even by police, but others such as New York and Massachusetts had laws – and still have – allowing police to tap under court approval. But approval is often a rubber-stamp gesture, and much free-lancing undoubtedly goes on, encouraged by the fact that federal prosecutors have been remiss in bringing charges against police officers. In New York City alone, knowledgeable observers estimate there are thousands of taps working at a given time. In *The Eavesdroppers*, Samuel Dash wrote: "One former telephone company employee, who frequently provided plainclothesmen with information they needed to install illegal wiretaps, reports that for every ten legal wiretaps installed by plainclothesmen with court orders, there are ninety illegal taps by plainclothesmen without orders." Dash extrapolated this to arrive at a figure of from 13,000 to 26,000 wiretaps a year. That this was a modest approximation is indicated by the testimony of a plainclothesman in a 1951 bookmaker's trial:

Question: Did you engage in wiretapping as a plainclothesman?
Answer: *I did any number of illegal taps – very few legal taps. Most of mine was what you would call an illegal tap.*
Question: You mean a tap without an order?
Answer: *Without a court order. In fact, I would not know how to go about getting a court order. But I can tap your phone for you.*

Over the years there have been numerous incidents of unscrupulous police using information obtained by wiretapping to shake down book-

makers and blackmail individuals. Recently, five New York policemen were charged with selling computer-stored information to private detectives.

But wiretaps are only a part of the electronic invasion story. The practice of bugging has proliferated of late, encouraged by the ready availability and low cost of microphone-transmitters. In a sense, bugs are more insidious than taps. Whereas a tap can be installed without violating the space of a home or business, bugs ordinarily require trespass — in the police argot, a "black bag job." In many areas bugging was not or still is not against local laws. Until the Cahan decision of 1955, California law officers carried on extensive legal bugging. In that milestone case Los Angeles police admitted that they had clandestinely entered the premises of Cahan, a suspected gambler, and hidden a microphone. The California Supreme Court toppled Cahan's conviction on the grounds that the interception constituted illegally seized evidence, and commented tartly that the police testimony revealed "they casually regard such acts as nothing more than the performance of their ordinary duties for which this city employs and pays them."

Bugging and wiretapping are forbidden by Nevada statute. But in 1966 a total of 22 bugs were found in Las Vegas casinos, connected to leased lines channeled to the local FBI office. No prosecutions were made. That an agency of the federal government chose to flaunt state laws may go a long way toward explaining why federal anti-eavesdropping laws have gone largely unenforced.

This permissiveness has spawned widespread electronic snooping outside of law enforcement.

There is a chronicle of prominent episodes. In 1955 in New York City it was discovered that a private detective firm specializing in divorce cases obtained access to some 100,000 telephones on the East Side by coopting a telephone company employee in a key position. In 1958 a government sleuth and newspaper columnist took a hotel room next to the suite of manufacturer Bernard Goldfine, due to testify about influence peddling, and slipped a bug under a common door. In 1965 Schenley Industries board chairman Lewis S. Rosenstiel disclosed that confidential business discussions had been tuned in on by a bug under the bar of his Miami Beach home. Also in 1965 former Alabama attorney general Richmond Flowers found a tiny three-wire transmitter in his telephone handset, shortly after announcing an impending probe of the Ku Klux Klan. In 1967 the president of a Southern California utilities company told a Senate subcommittee that a bug had been found in his desk. And in 1970 investigators found a mike-transmitter concealed behind paneling on a cruiser on which a San Francisco contractor and his engineers habitually prepared — and chronically lost — bids on large construction projects.

Perhaps the most off-beat tap was put in by a San Quentin Prison inmate in 1971. A repairman assigned to the prison's electronic shop, he tapped the warden's private line with a handset in the basement terminal box. Declared the State of California Corrections Director when informed: "I've learned that my so-called secret talks with the warden of my largest prison were not so damn secret after all."

Today there is a veritable army of men with

the technical capacity to install electronic devices and make surreptitious entry for that purpose. They have been trained and given experience by military intelligence at Ft. Holibird, Maryland, or the Signal Corps at Ft. Monmouth, New Jersey, by the CIA, which teaches tapping and bugging as part of its "Tradecraft" course, by the FBI in its "Sound School," by telephone companies, by private detectives passing on the trade, by self-taught electronics marvels, and by state and local police technicians.

In San Francisco in 1965 a police equipment company ran what it called the American School of Technical Intelligence whose curriculum ranged from the fine points of "audio surveillance" to "penetration," i.e. surreptitious entry. The students who paid $140 for the five-day course, included an Army intelligence officer and policemen. "What I learned in that course," commented one patrolman, "will keep me from ever pounding a beat."

Yet the field has also become infested with dillitantes attracted by the simplicity and low cost of some devices. Not long ago New York electronics expert John G. Marinuzzi obliged the Senate subcommittee probers by fabricating a miniature transmitter: "I built it at a cost of about $17. I bought the parts from a local electronics house . . . It worked quite well and was quite simple. I would imagine that any high-school kid, electronically inclined, could easily build it." As Robert C. Fogle, a consultant in the electronic security field, has put it, "Anyone with two dollars for the diagram, a soldering iron, and around fifteen dollars in parts can go into the bugging business. And present chances are ex-

cellent they won't get caught at it."

The Senate proceedings were also enlivened by testimony from Miami private detective John W. Leon, who sold kits called the "ten-day blitz" to skeptical spouses. Priced at $400, the kit included an easily installed telephone bug, a bug for the bedroom that could be attached to a voice-actuated recorder, and a bedroom-mounted movie camera that shot a frame at preset intervals. "At the end of a day you know everything that's gone on in the room," boasted Leon.

Electronic gear can be purchased as readily as any novelty item. The huge California mail order firm, Sunset House, advertised a "Private Ear" for $3.98. "Let's you be a silent party on the line or listen on an extension without lifting the receiver," the copy read. "No connecting wires of any kind. Just set the pocket-size unit beside the phone. It picks up and amplifies inaudible sound waves so you hear them on the earplug receiver!" A Los Angeles firm ran newspaper ads for a "Model 007 Micro Miniature Spy Transmitter" half the size of a matchbox and with a range of 200 feet for $85. A large New York supply house took display ads in *The New York Times* offering an FM pocket-size transmitter for $49.50 and a companion receiver for $39.50. And Senate investigators retrieved a two-transistor bug of unknown manufacture from a booth telephone that broadcast for a city block radius and could be made, they thought, for about $5.

The devices are billed as being useful for such innocuous purposes as electronic baby-sitting, party fun, and picking up the sounds of intruders. But one manufacturer admitted to the Senate subcommittee that he did a brisk business selling

This device picks up a signal from an extension phone by means of induction. Nothing is attached directly to the phone. There is no click to warn of its presence, and there is no signal loss.

to "the man who wants to act out his daydream of being a flesh-and-blood James Bond."[1]

On the following pages we will take a look at the devices and tools of electronic surveillance, how and by whom they are used, ways and means of detecting them, and how to take counter measures.

While an attempt has been made to touch all bases in the field, no volume can be wholly comprehensive. For the field of electronic surveillance is limited only by the eavesdropper's imagination.

[1] *This material can no longer legally be offered for sale for the purpose of electronic snooping.*

THE TELEPHONE TAP

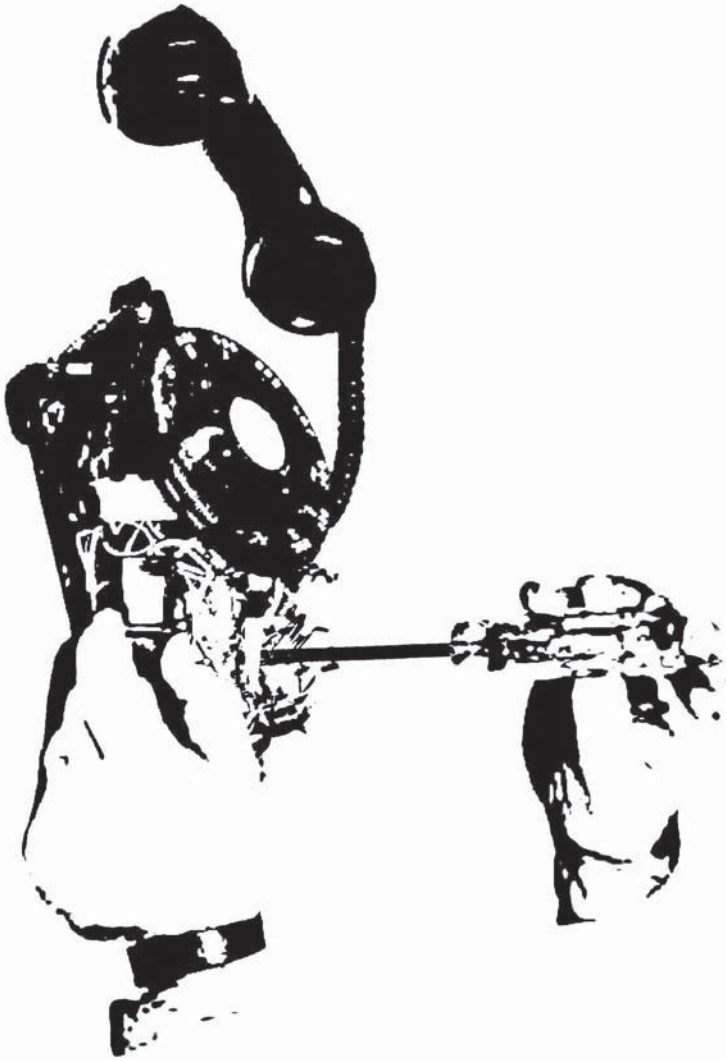
It may be appropriate to start by dispelling the myth that a telephone tap betrays its presence by clicks on the line. Only the most careless tapper would induce such sounds while the line was in use.

Although the public tends to use the terms wiretap and bug interchangeably, there are distinct differences. Wiretapping is the electronic interception of telephone, teletype, intercom, and other communication by wire. Ordinarily, it does not require trespass for installation. Bugging, on the other hand, utilizes a concealed microphone to pick up sound; the mike may be linked to the listening post by wire or be coupled by means of a wireless transmitter. Bugging usually requires trespass.

For the moment we will consider only telephone taps that intercept telephone conversations. Later we will deal with the various combination mike-telephone hookups that will intercept both telephone and room conversations.

By outlining how the telephone system works, we can see where it is vulnerable to tapping. From the standard Western Electric 500 or 300 series telephone instrument, insulated wire called the junction wire or station cord leads to a connector block in the room, then into the wall where it has been fished through to an outside connector block on the building. In office and apartment buildings it will proceed through floor terminal and distribution boxes and risers to a main frame, usually in the basement. A drop wire from the building delivers the pair of wires to a pole terminal box, where it is fastened to a pair of lugs, usually one of twenty-six such lug pairs. The pairs from the pole box then feed into aerial cable, which at some point drops into a subterranean cable main. This main leads to the telephone company central office, which houses several exchanges. There the individual pairs are soldered to a huge frame. When a number is dialed the switching equipment (line selector) establishes a connection between the dialing pair and the dialed pair, or routes the call down a trunk line to some other central office. On long-distance calls, the conversation is superimposed on a carrier generated by a RF oscillator; various frequencies are used to increase the traffic capacity, with band pass filters at the terminal city resorting them.

There are two principle types of tap: metallic or direct, and inductive. An induction coil picks



A tiny FM transmitter is being installed in this phone.

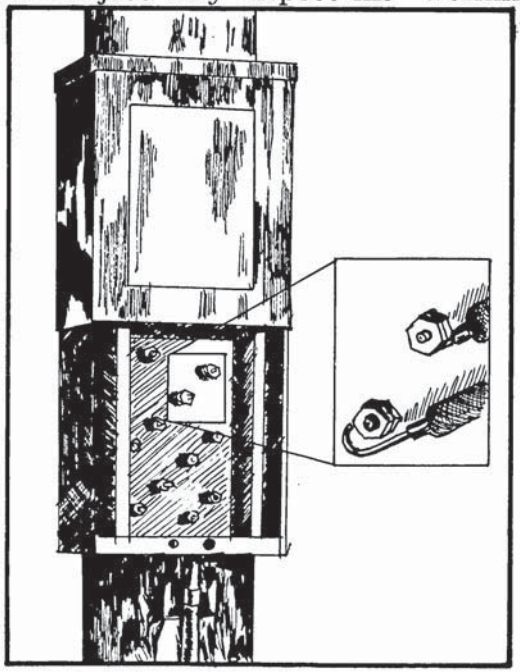
up conversation without any connection to the wire pair by "cutting across" their magnetic field. One preferred hiding place for the coil is proximate to the telephone instrument itself; the coil can be made in a flat configuration and placed under phone base or a desk blotter. Or it can be secreted inside the base to couple with the side tone coil, which along with a resistor is in the anti-sidetone circuit. The coil can also be placed parallel to the wire pair, any convenient place along its run from the instrument to the terminal box, provided it is within a couple of feet. In practice, this usually means placement behind a molding or wall interior. The induction coil finds frequent application in tapping public telephone booths.

The most marked advantage of the inductive tap is that it can be quickly placed and removed, making it useful in spot situations. Disadvantages are that the volume level tends to be lower and interference from AC sources is more likely. If the coil is placed at a point where the target pair has joined one or more other pairs, as happens in office buildings and apartment houses, the result may be a jumble of other phones simultaneously in operation. However, the tapper can preclude this by separating the target pair from the others.

A metallic tap means that the eavesdropper has fastened his own pair of wires to the target pair, a process known as "jumping" or "bridging." The bridge can be made anywhere the wires are accessible — the telephone instrument, the connecting block, or anywhere along the wire run to the terminal box. In practice, most metallic taps are made without committing trespass, either at the main frame of the office or apartment building

or the pole terminal box of a dwelling. The modes of tapping are varied. A simple one is to run a pair of very fine lacquered wires from the lugs in the pole box down the cracks in the wooden pole; the eavesdropper can drive up and clip onto the loose ends. A more elaborate and permanent rig consists of the eavesdropper stringing his wires from the lugs to a rented premises in the vicinity. Or he may tuck a wireless transmitter into the terminal box or hide it nearby. All of these arrangements are subject to discovery by telephone linemen.

Another security problem is posed by the proximity of the subject's premises to the pole box where the drop wire terminates. A surveillance-conscious subject may inspect his "working ap-

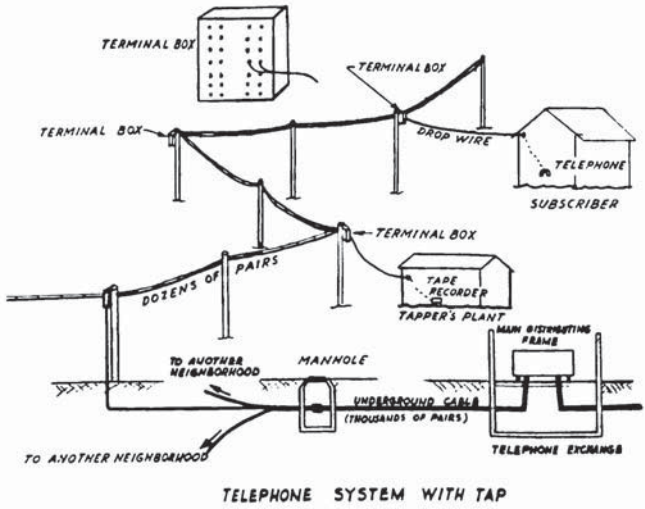


This diagram of pole terminal box shows how a "pair" is attached.

pearance" in the pole box for a bridge by climbing the pole, or he may be alert for irregular activity around the box. Consequently the eavesdropper may try to locate a "multiple appearance" a safe distance away. It is phone company construction practice to have one or more extra appearances of a particular pair in other pole boxes in order to allow for party lines. These multiple appearances may be anywhere within a mile or so radius. Their locations can be determined from the Cable Book and subscribers' Line Cards at the central office. Although the Book and Cards are supposedly confidential, federal agents and police usually can obtain the data, and private investigators may have contacts within the telco (telephone company) who will get it for them. A talented tapper can find a multiple appearance by a trial-and-error method called the ring-back system. Each local telco has a three-digit number that a repairman can dial in the field that will set the appropriate phone ringing. The tapper who knows the code can keep trying pairs until he gets the ring-back for the subscriber's number. He can cut down on the trial by training a practiced eye on the cable layout in the area and doing some educated guessing.

Tapping in an apartment or office building is not all that difficult. Some telcos unwittingly oblige by numbering the main frame according to apartments or office suites. But the line can be singled out by putting a tone on it near enough to the phone instrument that it can be identified back at the terminal board and then going "across" the pairs at the terminal or frame until the tone is heard.

For federal and police agencies the tapping op-



TELEPHONE SYSTEM WITH TAP

This diagram shows a telephone system with a tap on the line. The tap is in the pole box.

tions are greater due to the cooperative attitudes of most telephone companies. Although the regional entities of the Bell System function fairly autonomously, most will violate their own rules on behalf of law enforcement, especially federal agencies. In addition to supplying cable and card data, and looking the other way when taps placed by law enforcement are discovered by a lineman or repairman, the telco special agents may go so far as to place a tap feeding a recorder in the central office, or attach a dial pulse register to the line. From the number of pulses and their spacing, the number dialed can be reconstructed.

The phone companies also willingly furnished leased lines to law enforcement agencies desiring to feed taps to a central monitoring location.

Since the work order does not contain instructions for hookup at either end, the purpose is obvious. Leased lines are expensive and only the well-heeled agencies can afford many of them. The FBI has ordered lines under such dummy fronts as Federal Research Bureau and Henderson Novelty Co., and in Washington, when it apparently exhausted its reservoir of names, it simply called them "special test circuits." The leased lines afford the agencies a kind of security, since there is no way of tracing the lessee without phone company divulgence.

The 1965 hearings of the Senate Subcommittee on Administrative Practice and Procedure, then chaired by Senator Edward V. Long of Missouri, elicited just how the telcos answer government agencies' summons to duty. The Southwestern Bell hierarchy not only ran special lines into FBI headquarters on the seventh floor of the Post Office Building to facilitate tapping of suspected gamblers' phones, it dispatched its own men to go with disguised FBI agents and help them actually install taps. The company's division security supervisor, Arthur S. Brewster, acknowledged that he had worked hand in glove with the FBI "ever since I have been in this job."

Checking for a Phone Tap

Some people suspect a phone tap because information has leaked to competitors or adversaries, or because it is obvious that their movements are known in advance to adversary parties. In such a case it may be advisable to attempt confirmation by planting false information solely

The regular microphone of this receiver has been removed. It is being replaced by a microphone which also transmits to an FM receiver.

on the phone. If the reaction is noted as expected, the tap is confirmed.

Anyone suspecting a tap can lodge a request with the telco special agent's office for an inspection. But because they are responsible for such matters as telco security and fraud against the company, the special agents work closely with law enforcement. As a result they are not likely to disclose that a tap placed by law enforcement was discovered, and in fact may tip off the offending agency that a tap is suspected by the subscriber. Consider this exchange between Senator Long and Southwestern Bell's Brewster during the subcommittee hearings:

Long: You have found those (taps). What did you do with the equipment that you found?

Brewster: *Our instructions to our people are, who actually make the inspection, remove the equipment and give it to the customer and advise them to contact the law enforcing officers, preferably the FBI.*

Long: What would you have done if you got a call from the Acme Jobbing Company, I believe you said, down at 2512 McGee Street (one of the places Brewster's men had helped the FBI tap)? What would you have done if you had gotten a call that their line was being tapped?

Brewster: *I don't know, to be frank with you.*

Long: Would you have gone down to check it?

Brewster: *I just don't know.*

Evidently Brewster had never run into that kind of denouement. But since the Las Vegas debacle which resulted in the local telco being

sued for invasion of privacy and breach of contract, the telcos have been uneasy and might see fit to ask the tapping agency to remove it.

When the telco does do a check, it is usually two-phased. There is instrumentation at the central office that can determine if a particular line is unbalanced, subject to undue drain or contains hum or interference not attributable to natural phenomena such as crosstalk. For example, a tapper's leased line may cause a transmission loss, his recorder's oscillator may feed back a hum, or his recorder may cause a load on the line. But the professional tapper avoids these pitfalls. He uses a capacitor to block the 40-volt DC supplied by the central office batteries. He uses filters to block the hum. He uses a preamplifier or repeating coil on the leased line to preclude transmission loss. He uses a matching transformer to isolate the recorder from the line. These transformers are known in the trade as "black matchboxes," and are commonly available. Silmar Electronics of Miami, Florida, offers one at $17, while Fudella & Associates of Toronto, Canada, charges $24.50 for a model having "a compensating network to equalize to a degree the audio level of the local and distant voices."

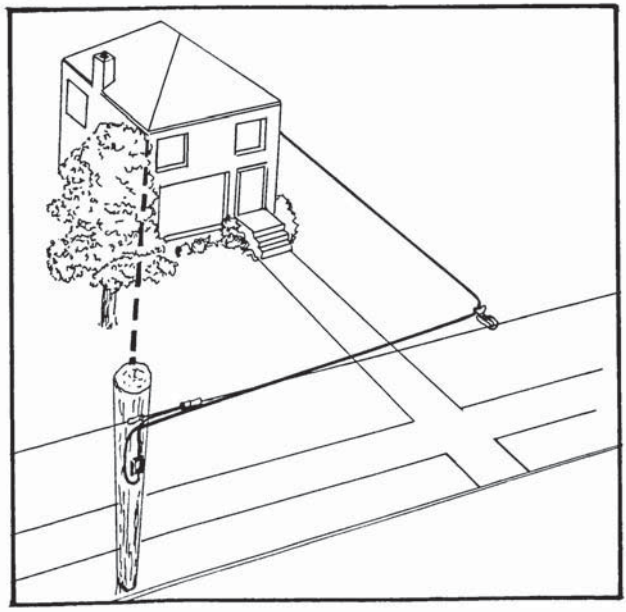
Sometimes a Wheatstone Bridge-type instrument will detect an altered line and roughly determine where the alteration is located. But if the tap is professionally installed, a visual check is the most practicable recourse. The telco will dispatch an employee to check a subscriber's line, in addition to conducting central office instrumentation surveys. But if a "foreign attachment" is found, the telco goes no further. As a public utility, it confines itself to verifying the presence

This a closeup view of an FM transmitter-microphone which fits into the telephone mouthpiece. It transmits both sides of the conversation and is powered from the telephone itself.

of a tap and removing it, thereby restoring the subscriber's privacy.

The victim can secure the matter further by filing a complaint with the police or FBI, since tapping is a criminal violation in some states and a federal violation under the Communications Act, which falls within FBI jurisdiction. What action he will get is questionable. FBI policy is to forward the facts of the complaint to the Department of Justice in Washington and do nothing further unless instructed. An alternative is to retain a private investigator versed in electronic surveillance to try to trace the eavesdropper.

A word of caution: the eavesdropper should not be prematurely alerted by placing calls to the telco, police, FBI, or private investigators on the



The telephone company sometimes uses a "run-out" to avoid interference (as from this tree) in reaching the terminal box on the pole.

line in question. Otherwise, it may not be possible to identify him. There are several steps that can be taken to this end. If he has strung his own pair of wires from the pole box, the wires can be physically traced to his monitoring site. If the monitoring site is tended only by automatic equipment, a stakeout can be mounted for when he returns to pick up tapes or replace batteries. The eavesdropper may also return to retrieve a transmitter or preamplifier inserted to boost the voice signal along a lengthy line, especially if it is expensive equipment. Should a jumper wire be found in the pole box, the eavesdropper most likely has connected to a leased line running to his plant. In the event the telco will not identify the lessee, a lawyer may be able to obtain a subpoena *duces tecum.*

Preventive Measures.

There are certain precautions a potential eavesdrop victim can take. Beware of bogus telco repairmen working on terminal boxes. Government and private tappers possess telco handsets, tool kits, linemen's climbers and belts and other authentic gear. Installers and repairmen are required to carry telco identification; inspect it carefully and call the central office if there is any doubt. And check their truck – it may just be painted similar to a telco truck.

Simple security checks can be made periodically. Check the small connecting block on the wall. Wires should run from the phone to this block. Remove the block and look for additional wires running from it into the wall. Check the

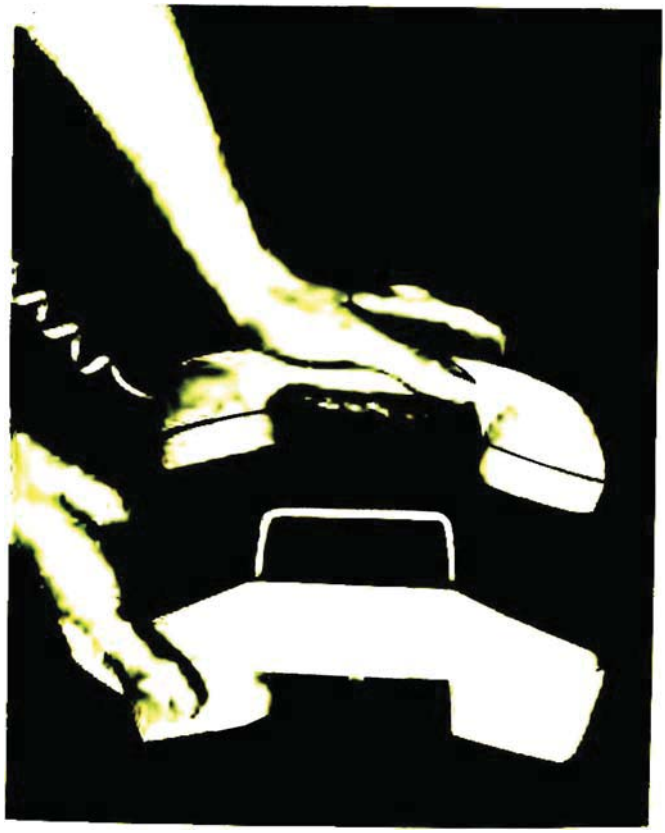
screws and terminals for scratch marks suggesting the use of alligator clips. Also check the wire along its run wherever accessible for breaks or cuts in the insulation that may be indicative of a sporadic tap.

Apartment and office occupants should inspect the main frame, usually in the basement, for alien wires, breaks, or altered wires. Telco installers and repairmen usually do not leave extra unconnected wires. The eavesdropper may be making spot taps using a rig as primitive as alligator clips and wires leading to headphones or a recorder. Most skilled eavesdroppers take the precaution of inserting a "black box" between the line and their equipment. The device is simply a capacitor and transformer to match impedences.

Inductive tapping can be thwarted by running the wire pair through shielded cable or conduit, and by locking all junction and terminal boxes and access panels.

Increasing numbers of business firms are buying security in the form of voice scramblers. When used by key personnel, the scramblers frustrate not only outsiders but switchboard operators and listeners on extension phones. The most popular model asserts that it "converts the sound of the human voice into unintelligible jargon which can be vaguely identified as the sound of an incomprehensible foreign language, similar to the effect of a phonograph record played in reverse . . . Only by the use of a matching instrument on the distant end is it possible to hear the reconstructed garble as clear speech. Instruments are especially coded so that instruments must be coded alike for use."

The scrambler contains its own batteries. In



This device is a speech scrambler. The receiver fits into it. The earphone unscrambles the incoming message and the microphone section scrambles the outgoing message.

use it is held against the phone handset by the user's grasp. The names of scrambler owners and their individual scrambling codes are secured in the manufacturer's safe.

The problem with scramblers using voice inversion is that an eavesdropper tapping the line can turn his amplifier all the way up and thus make the conversation intelligible again. Thus the scrambler is a privacy device – not absolute security.

A recent entry in this field is made in Switzerland and distributed in the United States. The distributor contends that no voice communication can ever be secure, but the crypto system can because it supplies about ten to the 38th power different basic programs. It has a built-in electronic computer, a full-sized keyboard, and an alpha numeric tape printer. It is fully portble. The enciphered messages printed out on the tape can be sent via teletype, radio, telegraph, telex, or mail.

WIRED MIKES AND BUGGED TELEPHONES

In 1965 an indignant woman called a San Francisco radio talk show berating previous callers who had expressed concern over the current snooping craze. She ran a motel, she said, and customers frequently defrauded her by bringing extra, nonpaying occupants into the room. To prevent this she had had all the rooms in the motel bugged. "We have a right to protect against cheaters," she insisted.

The woman's revelation set off a wave of outrage. How many motels were bugged in this manner? What sonic voyeurs were listening in? Disclaimers by the motel owners' association failed to reassure.

This tragicomic episode will introduce the topic of wired microphones and telephones converted into mikes, also known as "hot mikes." As has been mentioned, mikes – or bugs, as they are popularly called – pick up all conversation in a room, not just telephone talk. Under certain conditions the eavesdropper may *opt* to have a metallic connection to his listening post, just as the bugs in the motel undoubtedly fed into the motel office. Here is a case history as cited in *Machine Design:*

> The information leak was noticed almost as soon as it started. Somehow, the engineering secrets of the large West Coast company were getting to a competitor. Thinking it must be an internal leak, the company launched an investigation of personnel.
>
> After a year, with negative results and the leak still unplugged, the personnel director began to campaign for a professional countermeasure sweep. It took six more months before management agreed to this operation. The sweep was carried out and found a bug being used to bypass the hook switch on the telephone in a key executive's private office. This microphone, which drew its power from the phone circuit, had been continuously picking up all conversations in the office and transmitting them out of the building over the phone lines. The eavesdropper was never

caught, but the leak was finally plugged after 18 months and losses totaling near $1 billion.

The advantages of a wired bug as opposed to a wireless bug-transmitter are several. First, the fidelity of the signal tends to be higher, the stability greater, and the pick-up radius wider. Second, there is no need to trespass to replace batteries – the power can be supplied from outside. Third, the presence of the bug cannot be detected by radio locators.

The wired mike is highly desirable for permanent installations. This was the type the FBI used in Las Vegas. In the Fremont Hotel, for instance, an agent in the guise of a telco repairman entered the office of one of the executives and planted a carbon mike behind the baseboard. It had a plastic tube for acoustical impedance matching. It was hooked up to a leased line obtained in the name Henderson Novelty Company; the line led to the local FBI office, in which there was a central monitoring plant.

Frequently in these permanent-type installations the bug is buried in the wall. Obviously, whoever installs it must be a passable carpenter and plasterer, and have a kit with an assortment of paint colors.

On occasion the painstaking eavesdropper will make a binaural installation, permitting him to listen in luxurious stereo. The placement of two bugs properly spaced will increase in the intelligibility, but at the same time four wires are required instead of two.

Bugs buried in walls and plaster must have air conduction to function. Consequently, the eaves-

CROSS SECTION OF WALL

The FBI used this type of microphone in the Fremont Hotel, Las Vegas. It was discovered in 1965. The plastic tube carries the signal to the microphone, and aids in cutting down on hollow room noises and extraneous sounds. This system is called acoustical impedance matching.

dropper will leave a hole, although it may be so tiny as to escape all but the closest inspection. A typical installation would be a hole drilled in the baseboard to accommodate a plastic tube of ⅛ inch inside diameter; the tube travels entirely through the wall, mating with a conical flare that fits the mike face.

The eavesdropper can "borrow" existing wires to transmit the signal. The telephone pair, burglar alarm wires, the 26-volt furnace control system, doorbell wires, intercom lines, and AC power lines are all possibilities. It is also possible to reverse the role of a loudspeaker, making the speaker serve as a microphone. Thus public address systems are potential "in place" mikes.

The use of the regular power wires as transmission wires is fairly common, and is known as "wired wireless." A mike modulates a small oscillator in the low RF range, usually 20 to 200 KHz. The oscillator is attached to the 60-cycle power line via capacitors. The RF signal travels along the line and can be retrieved anywhere on the input side of the power company's distribution transformer. Because the signal is at such a low frequency, it is difficult to detect.

Another method of running wires from the target premises is in conjunction with the drop wire to the telephone pole box. Federal agencies have a source of supply for drop wires identical to the telco's except that they have a pair of additional fine wires built into the insulation. By replacing the original drop wire with this one, the mike output can be picked up at the pole box. At that point the fine wires can be connected to a leased line leading to the monitoring station. This is a favorite FBI installation.

Bugs available to the eavesdropper vary widely in size and performance characteristics. There are seven principal types: the carbon microphone, which is found in the mouthpiece of the phone handset and is alluded to as a "button mike"; capacitor mike; dynamic; sound-powered, or controlled reluctance; ribbon, or velocity; and crystal and ceramic, which rely on the piezo-electric effect.

Some firms put out bugs designed especially for eavesdropping. For example, a New Jersey firm offers the SB-2 (for sonic bug) which is about the diameter of a quarter. There is also a genre of subminiature bugs, most of which are manufactured in Europe and handled through the large distributors in this country. One company offers the famous Sugar Cube Microphone that measures only 5/16" x 1/4" x 1/8" and a flat subminiature mike that is only 3/4" long.

The conditions under which a bug will be planted and operated dictate the choice. The carbon mike is rugged and stable but requires relatively a large amount of power, ideally the 4.5 volts of three dry cells in series. While free of internal noises such as "hissing" or "clicking," high impedance mikes such as the crystal and ceramic must be connected to the amplifier or preamplifier via a relatively short wire run to avoid external noise pickup and signal voltage attenuation.

Amplifiers, or preamplifiers as they are termed if used to boost a signal along a line, are inexpensively available in radio stores and from bugging equipment suppliers. With the advent of transistors and printed circuits, amplifiers have been reduced in size and power requirements to a small package. A typical model used in bugging

is the Pocket Pal. It is not much larger than a pack of cigarettes, has low and high impedance inputs and outputs.

A doubly productive method of wired bugging is to convert the telephone into a bug. By doing so the eavesdropper not only can listen to telephone conversations with clarity and at both ends, but all other conversations occurring within a radius of the phone. Since telephones ordinarily are located within a few feet of where conversations are habitually held, the bug is ideally situated. The eavesdropper need only tap the phone line to tune in.

There are methods for combining wireless transmitters with the live phone mike, but for the moment we will talk about the wired variety.

In its rudimentary form the mike-tel, as the FBI alludes to it, involves bypassing the "off" switch in the telephone instrument so that the carbon mike in the mouthpiece is constantly energized. When a phone handset is lifted from the cradle, a spring-loaded switch closes the circuit, thus powering the carbon mike from central office batteries (which the telco calls the common battery system). At the phone the power level is 9.6 volts. The trick is turned by altering the wiring of the phone instrument, a complex operation requiring some 15 steps. The alteration must leave no more than 20 miliamperes drain when the handset is in the cradle, otherwise the line relay in the central office, which is set for about 40 miliamps, may be tripped.

A major drawback of this installation is that the four-conductor mounting cord, station cord, and drop wire must be substituted in order to carry the mike sounds away from the premises.

A variation called the single-pole mike-tel can surmount this problem. The SPMT unit, inserted in the line anywhere between the phone instrument and the central office, automatically switches the phone from mike to ordinary tap when the instrument is picked up. Then when the handset is cradled a reset button disconnects the central office and the unit supplies the mike voltage. The switch is jumped by a condenser and a resistor dissipating five watts; the AC impedance of the condenser is less than that of the resistor, allowing AC to pass while the resistor lowers the DC current.

Since mike-tels require time-consuming alterations of the phone instrument, the eavesdropper sometimes will simply substitute an already altered phone.

Some agencies also have a RF mike-tel that operates in the 27-120 kilocycle range. It is limited to 1000 feet effective operating distance. But the pair of wires should be twisted, and there cannot be long legs or multiples between the phone and the monitoring plant.

Possibly the most exotic of the wire mike-tel species is the "harmonica bug." The invention requires access to the target phone instrument, to which a switching device and mike amplifier is attached. The eavesdropper merely dials the number from his own phone, blowing a harmonica note of a specified frequency. It is most important that this tone be sounded prior to the first ring, activating the relay decoder circuit before the phone has a chance to ring. This has the same effect as lifting the receiver of the handset, preventing the phone from ringing, but establishing a connection so that the carbon mike acts as a

An exotic piece of equipment is the "Harmonica Bug".

room mike. The amplifier boosts the signal level.

The singular feature of the harmonica bug is that it will work on any phone on the direct dialing system, no matter how distant. "How close do you have to be to eavesdrop on a conversation in New York?" asks a catalogue in promoting its "infinity transmitter" version. "Try Los Angeles." What the catalogue doesn't say is that a trip to New York is necessary to install the switcher and amplifier.

A manufacturer told the Long subcommittee that he would sell this device to anyone, harboring second thoughts only if he suspected it was "going to be used for nefarious purposes."

Checking for Wired Mikes

As has been noted, mikes planted in walls, plaster, and behind paneling must have air conduction, however minute. Therefore a visual check of walls and paneling looking for air holes is a first priority. Signs of recent carpentry and plastering such as rough spots, unmatched paint surfaces, and inconsistent aging characteristics should be sought. A metal-detector type probe can be used to ferret out metallic devices behind walls and paneling, but some mikes are made of plastic or ceramic material to avoid just such detection.

Ducting systems are a prime hiding location and should be carefully inspected.

The most vulnerable aspect of the wired mike is its use of wires to convey sounds away from

the premises. A search for unexplained wires should be conducted. It should be pointed out that some years ago the telco went from four-conductor mounting cords and station wire to three. Although most connecting blocks in use have four terminals, only three are used. There is a red and green pair and yellow ground wire. Each premises is guarded by a protector block, which in homes is ordinarily mounted on an outside wall below where the drop wire leads away. This block contains a fuse to protect against voltage surges as might be caused by lightning. From it the ground wire is connected to a ground, and the red and green pair to the drop wire.

In seeking wires it should be borne in mind that conductive paint may have been used to carry the connection over spots vulnerable to visual detection.

The search should initially be localized to those areas where conversations are routinely held. While the sensitivity of mikes varies greatly, most cannot pick up intelligible conversation at over 20 feet, much less from another room.

Scrutiny of the telephone instrument is also in order. Attachments such as the harmonica bug should be readily identifiable, but altered switches and wiring is usually the province of experts. There is a "hot mike" detector on the market called the Snooper that incorporates an induction coil. By leaving the handset on the cradle and placing the Snooper in close proximity while speaking, one will hear his own voice coming through the device's monitoring system if there is a "hot mike" alteration.

Another technique is to examine walls, furni-

ture and other likely hiding places with portable X-ray equipment. This is a fairly costly procedure.

Since mikes are relatively small and easy to conceal, the search can focus on finding preamplifiers and batteries. Out-of-the-way spots in basements and attics are likely caches, as are pole terminal boxes. Occasionally an eavesdropper's aerial wires will pick up RF interference from nearby broadcast stations, in which case he will have to attach a low-pass filter that has been designed for the job.

If an installation is discovered, the problem of tracing is similar to that in wiretaps. If the eavesdropper has used expensive equipment he may attempt to recover it. If his electronic gear is unique, there is a possibility of tracking down its purchase. It should be kept in mind that conversion of a telephone instrument into a mike-tel is a violation of Section 605.

Preventive Measures

The same defenses as against wiretaps apply. In addition, it has been widely recommended that generation of a "white sound" such as by turning on the shower will mask the conversation. It is true that certain mikes will be neutralized by this tactic, but others will not. A radio may also be helpful.

To thwart the "hot mike," two additional contacts can be added upside down to the bottom of the stacked switches so that when the instrument is hung up they will form a short across the transmitter.

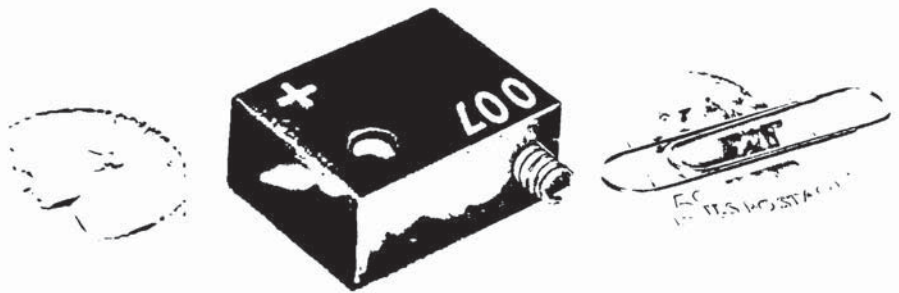
Another partial defense is to order a Touch-Tone phone from the telco. Not only is the Touch-Tone difficult to bug, it renders the "harmonica bug" device inoperable.

THE WIRELESS BUG

No area of electronic surveillance has become as romanticized of late as the wireless bug. In an appearance kicking off the Long subcommittee hearings several years ago, San Francisco private detective Harold Lipset displayed the olive-in-a-martini bug-transmitter, with the toothpick serving as an antenna. Other miniature bugs have been fitted into everything from cigarette packages to pens to diaries and Bibles. "Whisper Light," a decorator lamp, harbors a miniaturized bug-transmitter with a range up to 150 feet.

The plastic olive replica bug does exist and can be bought, although its usefulness is definitely limited. Most wireless bugs in use are far more prosaic — and practical. The dawn of the transistor age enabled them to be made more compact and draw less power, thus proliferating their use.

A distinct advantage of the wireless bug to the eavesdropper is the security it affords. Once planted, there is no physical link to him, and he is unlikely to be caught except through his own carelessness. He might be careless enough to leave identifying or traceable marks on the device. Or he might be heedless of the security of his moni-

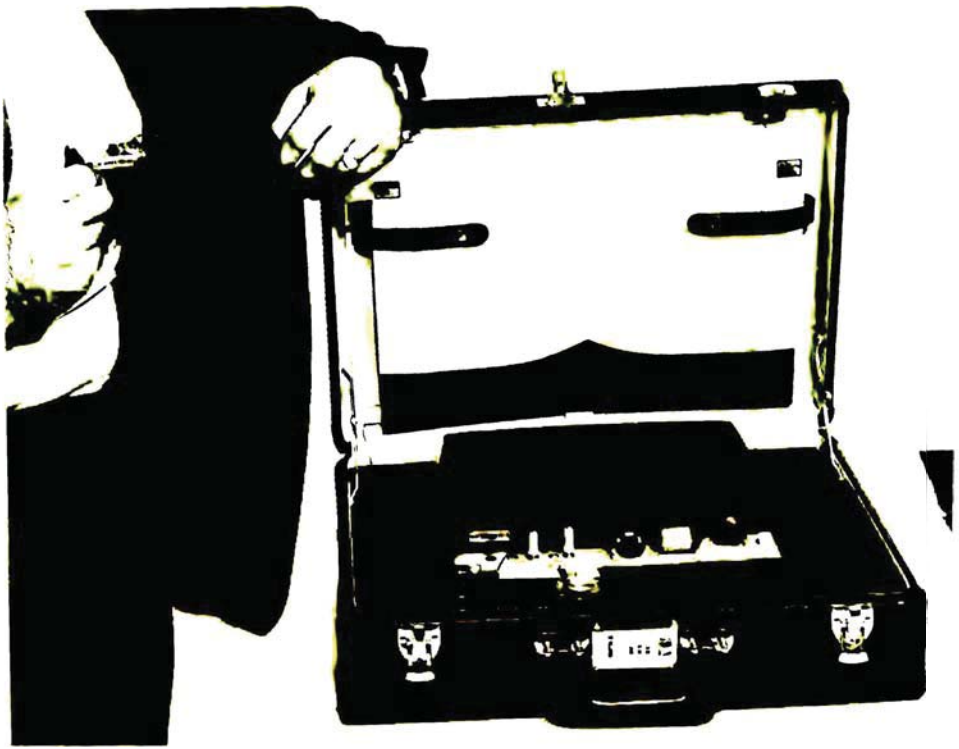


Despite its miniature size, this device is actually a complete FM transmitter.

toring post. A classic example occurred in Washington, D.C., in 1962. Attorneys representing a utility company in hearings before the Federal Power Commission occupied a suite in the Mayflower Hotel. A private detective firm taped a bug-transmitter under the coffee table in the suite. One of the attorneys, strolling down the hotel corridor, heard his colleagues in conversation. Not only had the detectives left the door to their room ajar, they used a speaker instead of earphones. By ignoring basic security, they found themselves discovered. They were prosecuted under the backdoor complaint of interfering with air traffic control communications, since there were no federal anti-electronic eavesdropping laws at the time.

One drawback of the wireless bug is that in nearly all cases a trespass must be committed to make the installation. Another is that the trespass ordinarily has to be repeated to replace the batteries. However, there are two general methods of avoiding trespass. One is to remotely activate the bug-transmitter so that it is in operation only when conversation is in progress, thus prolonging battery life. The other is to pirate power from an existing source such as power lines or telephone lines, thus eliminating the need for batteries altogether and permitting indefinite operation.

The first method involves the use of radio-controlled relays along the lines of those in remotely controlled model airplanes. A variation is to hook up a VOR (voice operated relay) to the bug-transmitter so that it *broadcasts* only when voices are present. Yet another is the use of a body capacitance sensor that functions on the



This wireless FM microphone is easily concealable. Its signal is picked up and recorded on the combination FM receiver-tape recorder placed in a secure remote location.

principle of elevator buttons, "feeling" the presence of the body and switching on the transmitter when a person enters the room and switching it off when he leaves. Theoretically, the radar sentry systems now relatively inexpensively available for home alarms could be converted to the same use. A bonus advantage of remote or automatic activation is that the chances of detection by microphone locators is drastically reduced.

One method of pirating established power is to use a step-down transformer from AC lines. Sometimes the transmitting device will be attached inside the television set, where it meshes with the other circuitry and draws power from the set. A favorite source is the telco central office battery power. Most parasitic bug-transmitters in this class are designed for installation inside the telephone instrument.

One stock model's range is placed at "⅓ city block under normal conditions." Since devices drawing power from the central office battery must be low-powered, their range is not too great. One company has gotten around this with a model for which they claim a range of a quarter of a mile This is achieved by using a small mercury battery as the power source, then automatically recharging it with a telco battery when the phone is off the cradle.

There is a family of transmitters that broadcasts only telephone conversations, being energized by telco battery when the handset is off the cradle. A Senate subcommittee investigator found a tiny bug designed to substitute for a standard phone part in a Miami phone booth. Dubbed the Beeping Tom, it broadcast about one city block and could be mass-produced, the in-

vestigator estimated, for about $5.

A manufacturer that caters to police clientele has a tube-shaped model that weighs only one ounce and sends its signal for one city block. Another markets its "Wireless Telephone Transmitter." Mounted inside the phone base, it has a range of some three blocks. Outside, "on the line with the antenna," the range is stretched to up to one mile. Still another manufacturer checks in with a model, touted as "self-energizing and has a useful range of over 2000 feet under ideal conditions."

The most interesting entry in this field is a bug-transmitter concealed inside a practically indistinguishable copy of the Western Electric carbon mike. What this means is that the device can be dropped into the mouthpiece of the handset in the few seconds it takes to unscrew and replace the cover. Imagine this scenario. An automobile catches fire in the engine just outside your house. The driver asks to use your phone to call the fire department. While you're watching the fire (which he has set with a little gas) he drops the carbon-copy mike in your phone.

There are also in-line telephone transmitters that are battery powered. Most run on 9-volt transistor radio batteries. Since the batteries need replacement, the eavesdropper very often will install the transmitter outside the dwelling or at the main frame of an apartment or office building. Some models are designed to fit in the telephone base. One does double duty, broadcasting both telephone and room conversations within a radius of 300 feet. Most in-line transmitters are quite compact – they require no mike.

The variety of battery-powered bug-transmit-

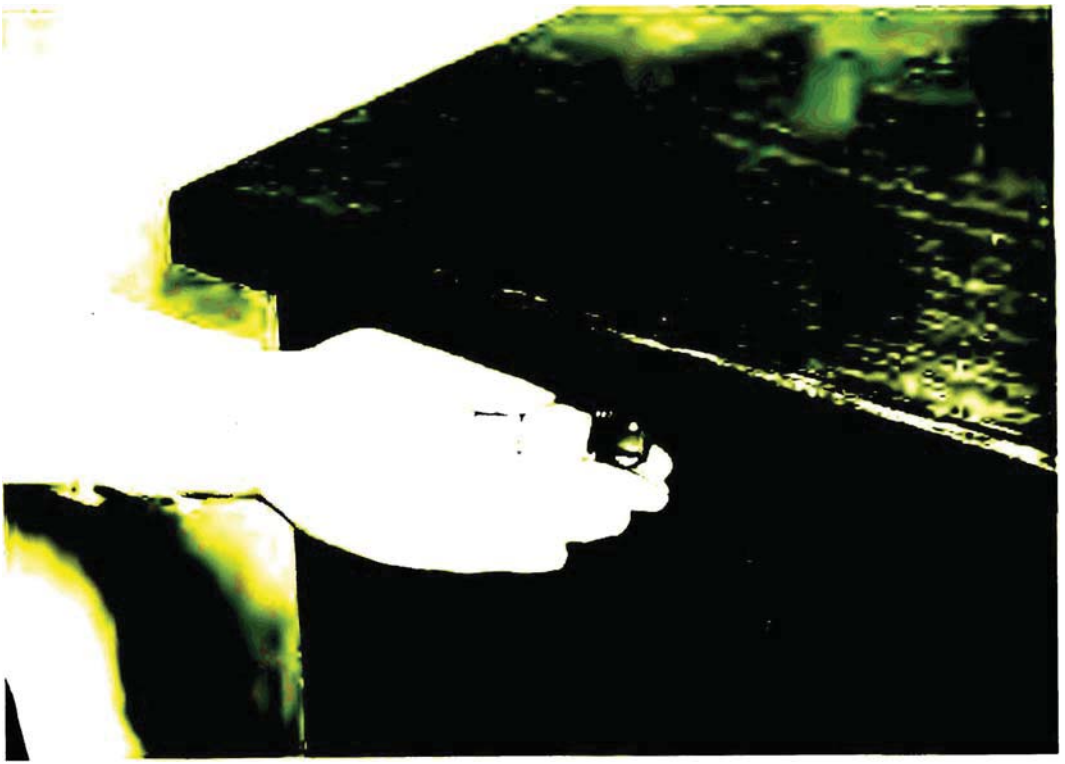
This easily concealed FM microphone and transmitter sends out a signal that can be received by a pocket FM radio receiver.

ters on the market is formidable. All but a few are FM, which produces less static and noise than AM. The wide price differentials reflect differences in mike sensitivities and the quality of components and circuitry, although the irregular nature of the market contributes to fluctuations for the same quality product. The eavesdropper has a choice between tunable transmitters and the crystal-controlled type. The tunable types provide greater flexibility in picking a frequency to operate on, which can be important when the eavesdropper wants to operate close to a commercial signal to disguise his transmission. On the other hand, the crystal-controlled is relatively drift-free and is virtually a necessity when the receiver feeds an automatic (VOR) tape recorder.

Development of the wireless mike can be traced to the need of the radio and television industries to eliminate wires snaking behind performers and producers. They are still used for that purpose. As used for broadcast and public speaking applications, the mike is usually looped around the neck, with the transmitter hitched to the belt or a shoulder sling or even pocketed. Mike-transmitters designed specifically for eavesdropping will usually have the mike built into the unit. The batteries may be inboard or outboard.

A major manufacturer of hi-fi and recording equipment offers a model which is crystal-controlled at 42.96 MHz, and a companion tunable receiver not only is of fine quality but contains an audio amplifier rated at five watts. The eavesdropping potential of this rig is formidable.

Inexpensive models, popular among private investigators, have self-contained nine-volt transistor radio cells. One was displayed by the Long



This FM transmitter can be quickly stuck to the underside of a desk—even with as common a substance as chewing gum.

This cuff link is actually a tiny microphone. The wire runs inside the shirt sleeve and plugs into an FM transmtter in the inner coat pocket.

subcommittee in a Newport cigarette package.

Bug-transmitters fabricated especially for eavesdropping tend to be even more compact and usually have a beefed-up audio stage. One pocket transmitter has a purported range of one-quarter mile. A feature of this model is that it can be powered internally or externally by means of a jack, thus exponentially increasing its battery life.

Perhaps the most famous — or infamous — of the micro-miniature groups is the 007. Its manufacturer at one juncture took out display ads in newspapers, touting its use as baby sitting and intrusion protection. Another manufacturer also spoke of noneavesdropping uses: ("Makes an excellent wireless microphone for use with P.A. system or dictating machine"), but in other ads it billed the device as a "latest scientific innovation to satisfy the spy in you." Measuring only 1″ x ¾″ x ¼″ and working off a 1.5 volt hearing aid battery, the 007 was obviously meant to be the ultimate in inconspicuousness.

The penultimate seems to be in the near future, and will be made possible by the technological breakthrough of integrated microcircuits. Formed by depositing metals and exotic materials in layers less than 1/1000 of an inch thick, these electronic "sandwiches" are so minute that it would take about one hundred of them to fill the area of a postage stamp. Even though they can do just about everything a transistor circuit can do, they need no power supply, drawing their energy from the ambient radiations of commercial broadcast stations. Already they are in use in aerospace and military applications, and federal agencies most likely are experimenting with them in snooping. Should they go into mass production,

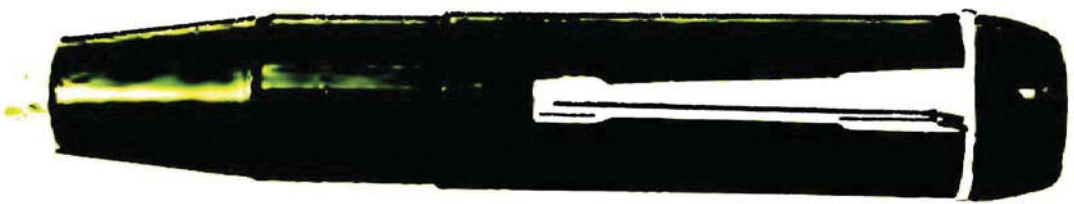
they will be as disposable as Dixie cups. Detection, either visually or electronically, will be extremely difficult.

Before the enactment of the 1968 federal law against the manufacture, possession, and advertising of devices primarily useful for eavesdropping, there were some 120 firms actively promoting such wares. The fact that the law is now on the books is no cause for assurance, however. The manufacture of devices whose primary use can be claimed as other than eavesdropping goes on. And there always has been a legion of free-lance fabricators, electronics experts who work for, say, aerospace companies and derive extra income assembling devices for private detectives. In Dallas recently, for example, a compact transmitter attached to a phone pair was found in a pole box. Investigation determined that it had been placed there by a private detective. The detective had coopted an engineer for a large electronics firm to design and build it. The device was extremely sophisticated, and transmitted in the 400 MHz band, far too high to be detected by most receivers.

Checking for Bugs

There are certain steps that the layman can take to detect hidden bug-transmitters. However, a check affording any degree of assurance that the premises is "clean" can be done only by experts with costly equipment.

A first rule is: look a gift horse in the mouth, carefully. Many a bug has been unwittingly welcomed when built into gifts such as picture



What appears to be a fountain pen in a pocket is actually a sensitive microphone feeding a concealed FM transmitter.

frames, desk sets, clocks, watches, pens, lamps, cigar humidors, cigarette lighters, and even artificial flowers. One source vends a framed wall picture with a bug-transmitter built into it. The pictures range from seascapes to still life.

A visual search for bug-transmitters can proceed along the same lines as for a wired bug. The telephone instrument and connecting block are distinct possibilities; some current pirating bugs are built into connecting blocks. Look for the aerial that each bug must have. It should be remembered that the mike, transmitter, and power supply need not be in one package. For example, a tiny mike could be concealed in a wall or anchored to a light switch, with fine wire leading to a safer or more accessible cache for the transmitter and batteries.

Since the smaller transmitters have a limited range, the eavesdropper's receiving site must be close by. He may have rented quarters, or use a vehicle. Police agencies and many private detectives have panel trucks or vans that look like business or utility vehicles; they are used for stakeouts and surveillances as well as mobile monitoring sites. It is also possible that the eavesdropper has hidden a receiver-recorder in bushes, underground, or in some other natural concealment. In the Redwood City industrial espionage case cited earlier, the mike fed a transmitter hidden in the bushes. Also in the case of short-range bugs, the eavesdropper may hide a repeater station close by that picks up the weak signal and boosts it to a monitoring site some distance away.

If a bug is suspected, a mental inventory should be made of salesmen, repairmen, and deliverymen who entered the premises recently. The

Both of these FM transmitters are disguised — one in a lipstick container and the other in a cigarette package.

search can then be concentrated in those areas accessible to them. Beware of persons gratuitously showing up to repair the telephone or inspect the wiring and construction for conformance to codes. They could be imposters.

Turning to the electronic means of detection, Continental Telephone has a meter-deflection device called the Private Sentry which it represents as a bug "detector." The probe is simply touched to any metallic part of the telephone base. It seems that this detector is actually a sensor of "hot mike" alterations and in-line transmitters.

The interception and identification of the clandestine signal is a principal method of detection. Obviously, a one-shot sweep cannot be considered thorough because the bug may be remotely or automatically activated, and if not broadcasting when the sweep is made will be missed.

Perhaps the simplest technique is to use a field strength meter to indicate the radiation. In its most elementary form the field strength meter consists of a crystal diode circuit with a meter whose pointer swings to the right when sufficiently close to a transmitter. No batteries are required — the ambient radiation causes the needle deflection. However, most meters have a potentiometer to regulate the meter input and a battery-powered high-gain transistor stage to ensure that the weaker signals are picked up.

A companion type of instrument that can be used for detecting transmissions is the absorption wavemeter. Most will cover from 2 to 260 MHz. When tuned through the spectrum, the instrument will resonate with the emitted frequency

The equipment laid out in this photograph demonstrates the array of electrical debugging devices necessary to detect today's sophisticated electronic snooping devices.

and indicate that frequency. Employing a grid-dip meter with its oscillator turned off will give the same results. The two are used in radio and TV repair work to detect spurious oscillations and as a relative indication of power in various transmitter stages. They are distinguished by a cylindrical protuberance, which houses the induction coil. Their cost is relatively low.

There are adaptations of these instruments designed specifically for bug detection.

One sports a probe and a speaker putting out "clicks" as well as a meter. Separate RF probes are available in stores that pick up from 100 kilocycles to 100 MHz. Radio stores also have field strength meters running the gamut from about $10 to $200, depending on their sensitivity. Some amateurs wire together their own with inexpensive components.

It should be kept in mind, however, that RF probes and field strength meters are for short range work only, their main use being in pinpointing the mike-transmitter once the fact of clandestine emission has been established. In the case of a field strength meter, the closer to the transmitter the greater the needle defection becomes.

A variation of the field strength meter substitutes a speaker for the meter. Several stages of amplification are introduced to produce a signal volume sufficient to cause feedback and its characteristic squeal. Most feedback-type devices have a jack receptacle into which an earphone jack can be plugged. The searcher then creates his own noise by whistling, humming, or stomping and moves in the direction the noise becomes louder in his earphones. A Southern manufacturer

has taken ads in trade journals read by corporate security officers for its model. This is a device anyone can learn to become proficient with, and its cost is not out of sight.

Another method is the tunable broad-band receiver as an interceptor of the clandestine signal. Most bug-transmitters are set to operate between 30 and 120 MHz FM, so that the band spread should be at least through this spread. The most popular bands are 30 to 50 and 88 to 108 MHz; the first is a standard shortwave band and the second is the commercial FM band, which means that the eavesdropper can readily obtain his receiver for these frequencies. The searcher using commercial receivers, however, should be aware that the eavesdropper can adjust his to receive slightly above or slightly below the standard band by trimming the oscillator padder.

To detect in-line transmitters and parasitic telephone transmitters, the phone handset can be removed from the cradle and a repeating time signal or weather report dialed. Then the receiver is tuned through the entire spectrum in quest of the dialed report.

In searching for room bugs, the idea is to first pick up the carrier, then determine what is modulating it. Regular citizens' band, mobile communications, ham radio, police, and fire department transmissions and similar broadcasts are intermittent, as required. Consequently the presence of a steady carrier suggests a bug.

At this point the signal must be analyzed. One way is to note the information or conversation being broadcast. If no modulation is present, the searcher can go from room to room creating his own sound. And if the signal is especially strong,

as opposed to the relatively weak signals of commercial radio and television stations, a nearby transmitter is indicated. Yet another indication that the transmitter is clandestine is the presence of harmonics. A harmonic is an undesired multiple-frequency emission of the fundamental frequency. Take a bug-transmitter operating on 88.5 MHz. It will put out a second harmonic at 177.0 MHz and a third harmonic at 265.5 MHz. With each harmonic the strength weakens. If a searcher discovers a transmission on 108.5 MHz and finds that there are harmonics, it is undoubtedly a clandestine transmission since the FCC requires broadcasters to employ equipment designed to eliminate harmonics. Most bugs are not so designed.

The fact that harmonics are common to bug transmissions can be useful to the searcher whose receiver is limited in its bands. Say the receiver is a standard FM broadcast radio with its band width slightly stretched. If the bug is transmitting on 50.0 MHz the receiver will not pick up that frequency. But it will pick up the second harmonic of 100.0 MHz.

Another improvisational bug detector is the common television set. When the set is warmed up, turn to Channel 2. Replace any outside antenna with "rabbit ears." Turn the fine tuning knob to its extreme counter-clockwise position, which brings the frequency to about 54 MHz. By rotating the fine tune knob clockwise the frequency is advanced to approximately 60 MHz. The searcher roams the room with the rabbit ears, watching the screen for a herringbone pattern and listening for the feedback squeal as the 6 MHz band is swept. He then goes on to Channel

3, whose low end is 60 MHz. All U.S. television channels are 6 MHz in width. Thus by repeating the process through Channel 6, the spectrum between 54 and 88 MHz can be investigated. Beginning with Channel 7 the frequency jumps to 174 MHz. Repeating the process now through Channel 13, the 174 to 216 MHz spectrum will be covered. From here the UHF band can be covered. Beginning with Channel 14, the low end of which is 470 MHz, the spectrum can be covered in six MHz increments to Channel 83, which is 890 MHz. Although it is rare to encounter a bug transmitting at this high a frequency, there is always the possibility of picking up a harmonic of a lower frequency.

Once a bug has been detected and its location approximated, the search can be narrowed further by using a probe. One of the most popular is the "magic wand" diode probe, one version of which looks like a slightly oversize ping-pong paddle.

Once the bug is found it should not be assumed to be the only one. Eavesdroppers sometimes plant a decoy bug, especially if the victim is security conscious. When it is found a false sense of security is induced, for a second bug has been planted. The game can be played both ways. If a bug is found it can be left in place and false information fed into it.

The identification of a bug is not always easy. Some bugs built solely for sale to law enforcement will bear manufacturers' names, serial numbers, or some distinctive mark. But most simply are not identifiable by inspection. Some professionals can identify a bug by its general characteristics and the frequency it operates on. But

who purchased it is something else again. Few manufacturers or dealers keep adequate records, or if they do are reluctant to give out the information. Sometimes an expert can recognize the handiwork of a particular craftsman, or the type of bug used by a particular agency. But with the proliferation of sources today, most bugs are simply untraceable.

Should a bug be belatedly discovered, an assessment of how long it has been transmitting — and what damage has already been done — can be gained from the remaining battery life. The device can be allowed to run its course to exhaustion, or a computation can be made by a technician based on the power it draws.

Preventive Measures

In many United States embassies in Communist-bloc countries there are special rooms within rooms called "fishbowls" that are electronically shielded and devoid of all wires. All furniture is either transparent plexiglas or molded plastic, without upholstery. In the so-called "mother room," which houses the fishbowl, are "white sound" generators giving off a howl of 75 decibels or so. It is inside the relative quietude of the fishbowls that the most important discussions are held, theoretically immune from prying ears.

Some industrial firms have followed this lead, installing their own fishbowl-like rooms in headquarters. But fishbowl rooms are not only costly, they are inconvenient and unduly restrictive. They constitute a high price to pay for escaping audio surveillance.

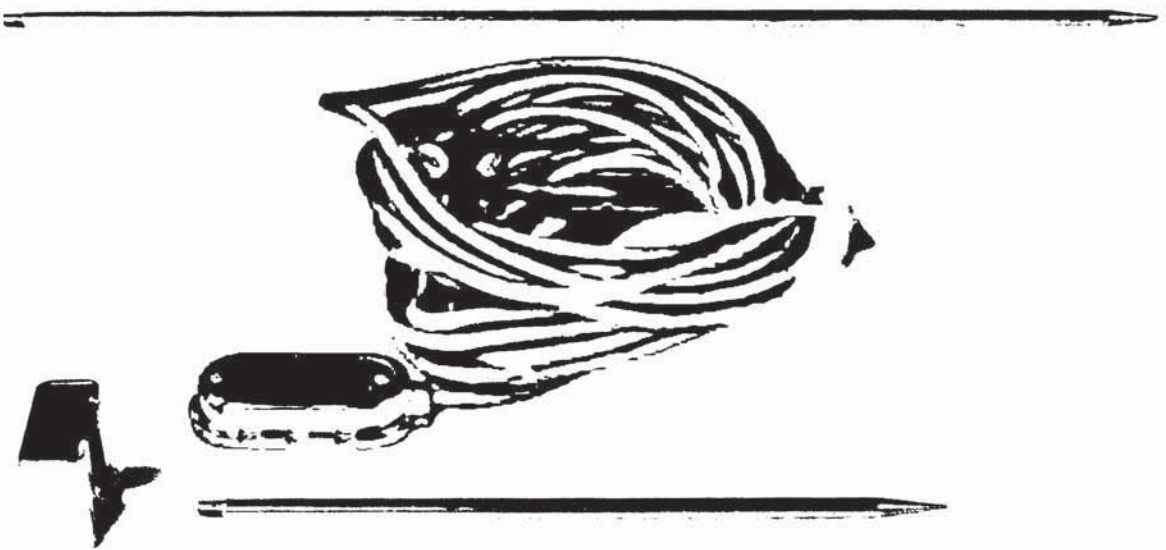
One countermeasure that is portable and modestly priced has gained some acceptance in recent years – a radio jammer. One model can be carried in the pocket. A prominent manufacturer sells a "Bug Eliminator" that can work off a battery or a power receptacle. Another has a dual jammer-line surge unit that throws hash at transmitters and wrecks mikes attached to metallic taps.

The jammer principle, however, is only a half-a-loaf countermeasure. For one thing the devices don't blanket all frequencies, and if they function at a power output sufficient to do a good job of jamming transmitters they are likely to cause RF interference on neighbors' TV and radio sets.

One practical device on the market is the "beep light." Apparently working on the field strength meter principle, the device actuates a red light when a transmitter is in the vicinity. The sensitivity is so adjusted that normal commercial broadcasting will not trigger the light. The beeper light is particularly valuable as a means of thwarting the briefcase transmitters now on the market in abundance. The briefcase "forgotten" by a visitor has picked up more than one ensuing conversation in the office.

THE ROOM NEXT DOOR

There is an assortment of portable listening devices designed for quick and easy eavesdropping without tapping telephone lines or making trespass. As Justice William O. Douglas has



This spike mike is driven through the wall into the opposite room to pick up conversations from that room and feed them to an amplifier or tape recorder.

described the situation: "With modern electronic devices, conversations within the home and the office can be made public without a key being turned or a window being raised. And those who listen may be private detectives and blackmailers, as well as law enforcement officials."

One widely employed device is the spike mike. Rather than picking up sounds through air conduction, the spike mike "hears" through the vibrations of the solid surface into which it has been driven, such as a wall, a door, and heating ducts. A large company offers a "high precision, high impedance" model instructing: "Simply insert into plaster wall (behind picture), sit back and relax." However, the majority of spike mike installations are made by drilling a hole in the outer surface of the wall, then poking the spike through so that it penetrates into the inner surface. The minute vibrations are transmitted by the spike to a mike-amplifier tandem, and the reconverted sounds are ordinarily loud and clear.

A class example of the spike mike in operation occurred in the District of Columbia in 1960. Police and IRS agents suspected that one Julius Silverman was conducting a gambling setup in his home. In turn, Silverman's attorney suspected that law officers were electronically eavesdropping. The attorney, Edward Bennett Williams, has recounted: "We carefully inspected the party wall of the house next door and we found a small hole under the molding in an upstairs bedroom. The spike fitted this hole perfectly. We looked at the blueprints of the building and discovered that while the wall was twelve inches thick at that point, it was not the solid wall it appeared to be. Inside the wall was a heating duct which supplied

hot air to Silverman's house. By pushing the spike microphone up against that heating duct, the police had obtained a perfect sounding board . . . The heating duct had been converted into a giant transmitter of sound and the heating registers of each room had become microphones."

The Supreme Court overturned Silverman's conviction on the fine point that because the spike was pressed into his heating duct a trespass had been committed. It failed to rule on what the case would have been had the eavesdropping been conducted without this trespass, such as can be done with the contact mike.

The contact mike is pressed against a surface but does not penetrate it. The Vibra-Mike is representative. An exotic entry in this sweepstakes is the pinhole/keyhole microphone with a long rubber acoustical tube that is nicknamed "the snake." The catalogue declares: "Poke it through a door, the slightest crack, send it over a wall or get daring and unreel it like a fishing line out the window. It can get to where you couldn't go yourself."

The stethescope mike is primarily used for listening through walls. It is similar to the doctor's instrument except that a high-gain amplifier is inserted between the pickup cone and the earset or recorder.

For intercepting conversations outdoors at a distance, the shotgun mike and parabolic mike are standard fare. The shotgun, or tubular mike, was developed over three decades by the Bell Telephone Laboratories. The most effective of these devices is a bundle of fifty small-diameter aluminum tubes varying in length from slightly over one inch to five feet. The tubes feed a com-

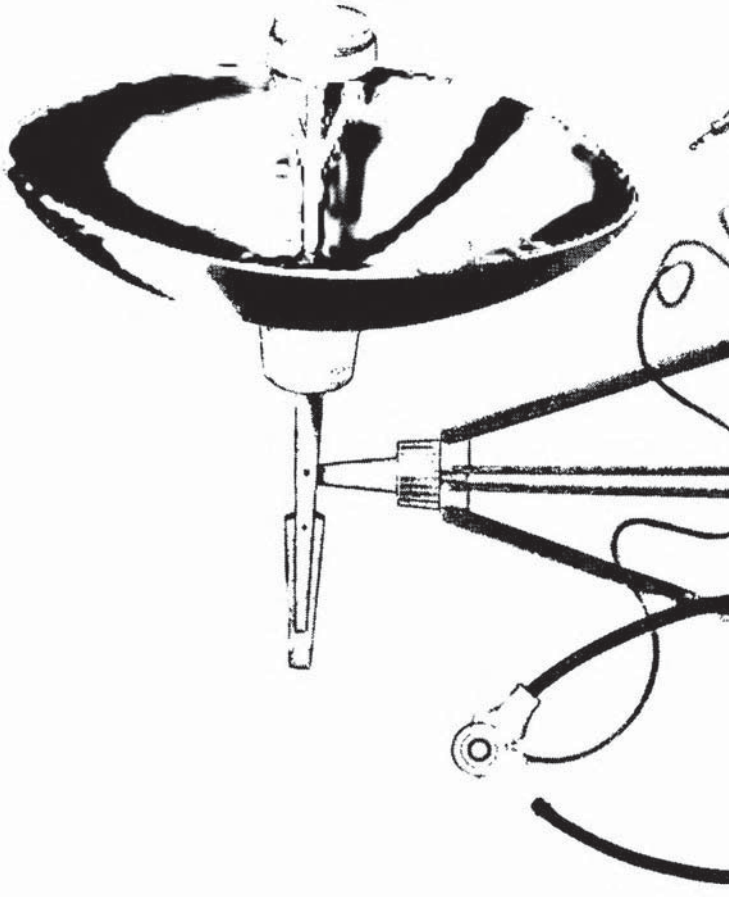
The shot gun mike literally focuses in on distant sound, much as binoculars bring distant objects clearly into view.

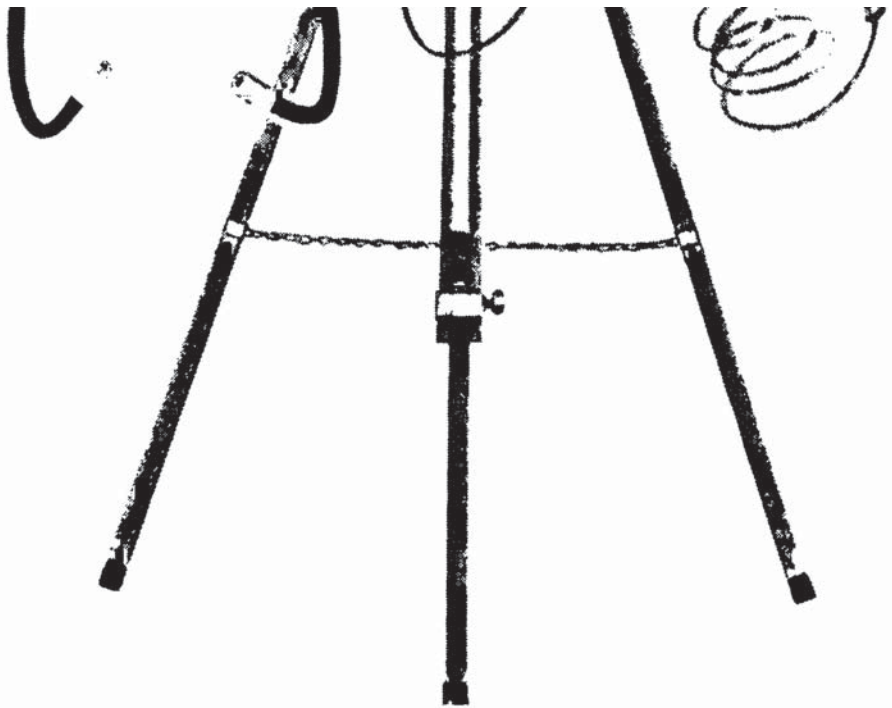
mon mike housing. The shotgun mike is highly directional and must be aimed like a gun at the target. The sound waves originating from the target area resonate in the tubes, reinforcing each other at the mike end. By the same token, sound waves from other sources arriving obliquely cancel each other out in the process of phase interference. Several years ago an ABC television special on eavesdropping showed two men conversing in a rowboat in the middle of a small lake, unaware that their talk was being taken in with great clarity by a shotgun mike concealed in a clump of bushes on shore.

One firm sells a version of the shotgun mike that seems to be an adaptation of the directional mikes used in studio sound work for such purposes as catching comments from someone in the audience. It looks like an oversized long-barreled pistol. "Two different size barrels, for very specific aiming," reads the copy, "with built-in wind screen for outdoor use." The wind screen is quite important, for it prevents noisy wind rush across the muzzle.

The "Big Ear" . . . The Parabolic Mike

More visually obtrusive are the parabolic mikes, with a reflector shaped like a dish. They have varied utility in industry and broadcasting, such as picking up the sounds of football battle for TV audiences. The parabolic mike also is highly directional. Sound waves from the direction in which it is pointed are reflected from the surface of the dish to a focal point at which a mike is mounted. Sound waves from side directions will





The highly directional parabolic microphone is visually obtrusive, but effective in certain specific applications such as on roof tops or across air shafts.

not be focused and therefore will not be heard. The effective range of these devices depends on a number of variables, among them the size of the dish, the character of the sound, and the extraneous noise level. Fairly effective models were advertised in *The New York Times* and *Esquire* for prices to fit every man's budget.

Preventive Measures

Since this family of listening devices is portable and used mainly in hit-and-run fashion, detection is difficult. If the eavesdropper has rented a room next to his target's, he has purchased himself a large degree of security. There is no practical or legal way to catch him with his contact mike against the wall.

The only defense against the shotgun and parabolic mikes is to look for them visually. Their size makes concealment difficult.

But since detection is an elusive quality, concentration should be on prevention. One simple but expensive strategem is to rent the rooms on both sides of the room to be occupied, thus ruling out common wall eavesdropping. A less than satisfactory measure is to observe the occupants of adjoining rooms as they come and go, since operatives and agents often are recognizable for what they are.

Federal and police agencies are in the habit of placing mikes in the walls of certain rooms in hotels and motels in major cities, leaving wires to be connected to from the adjoining room. Then a cooperative management, notified in advance by the agency, assigns its special guests to these

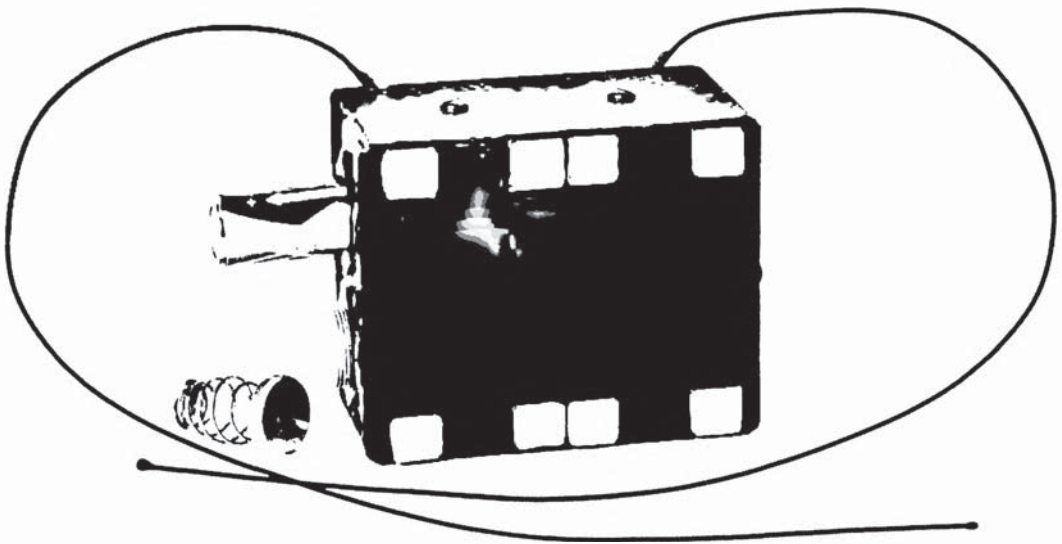
sonic studios and reserves the adjoining room for the agency. The best way to short-circuit this tactic is to insist on a different room than originally assigned.

THE BUMPER BEEPER

A homing device known generically as the Bumper-Beeper is often utilized by investigators desiring to maintain a "discreet" tail on a subject driving an automobile, or keep from losing him in heavy traffic. The Bumper-Beeper is simply a transmitter or oscillator attached to the subject's car that emits a steady or pulsating signal for tracking purposes. The name Bumper-Beeper originated with the frequent hiding of the device on the inside surface of the bumper.

A vintage model of the Bumper-Beeper was described by Jacob Fisher in *The Art of Detection* (1948): "The investigator makes a rough radio sending set with the aid of any radio repairman by attaching a small dry-cell battery to a vacuum tube. The entire mechanism fits into a cigar box . . . The investigator waits for an auspicious time when he can be undetected and attaches the contrivance to the axle or other unnoticeable protuberance of the subject's automobile . . . The shriek set up by the vacuum tube in the subject's car will be picked up at full strength by the loop antenna. When the noise vanishes suddenly it means that the subject car has made a turn . . ."

Although the Bumper-Beeper of today appeared in the James Bond movie *Goldfinger* as a kind



This external magnetic homing device attaches to the underside of the car being followed by means of magnets. It sends out a beeping signal, making the car easy to track.

of exotic gadgetry, it is really quite prosaic. The circuitry required to give off the audio tone or series of beeps (usually spaced 2 to 5 seconds apart) is not complex, and one unit advertised is only ¾" x 1½" x 1¾". To avoid the problem of battery dissipation on prolonged surveillances, some models can be connected to the vehicle's electrical system. The FBI has perfected a small unit – and this gets closer to James Bond – that when dropped into the gas tank will continually energize itself by chemical reaction with the fuel. The Bureau has found this unit ideal in its on-going surveillance of United Nations delegates and personnel in the heavy traffic of New York City.

How Bumper-Beepers Operate:

The range of standard Bumper-Beepers varies from less than a mile in downtown areas to more than five miles in open country. Some models are tunable, others crystal-controlled. Some attach themselves to metal by means of Alnico magnets, others must be attached by fasteners. One model is magnetically mounted, broadcasts a continuous tone on 49 MHz, boasts a range of up to three miles, and contains its own batteries. Another emits a pulsating tone tunable in the 30-50 MHz band, works off the 12-volt car battery and uses the car radio antenna to broadcast; it has a range up to two miles in cities, and is priced at $225.

There are several methods used to track a vehicle with a Bumper-Beeper attached. The roughest is to simply tune in on a receiver and follow in the direction of the strongest signal, a

somewhat flaw-prone technique. With two tailing vehicles, triangulation can be used. It is most desirable in any case to have a radio direction finder (RDF), which consists of a radio receiver with directional antenna and signal strength indicator. As the loop is rotated, the signal passes through positions of maximum and minimum strength. Maxima occur when the loop is end-on to the beacon, and minima when it is broadside. Crude but satisfactory RDF gear designed for small boats can be bought for as little as $150.

Another technique is to mount a second antenna on the vehicle doing the trailing, feeding its output to the receiver in such a manner that when signal strength is the same at each antenna they will cancel out, leaving a greatly attenuated signal or null zone. Thus, if the antennae are mounted exactly opposite each other, there will be a null zone when the vehicle is pointed in the direction of the subject's. Still another is to mount three antennae of varying length, feeding their output into the receiver via a three-position switch. By switching antennae and noting the varying signal strengths, the distance can be gauged. Sometimes a field strength meter or "S" meter is connected to the receiver to visualize the varying intensities. The above two techniques obviously require a practiced operator.

If the investigator has knowledge of the general area into which his subject is traveling, he need not conduct a moving surveillance but can seek out the beeper after the subject has reached his destination.

Anyone suspecting his vehicle is fitted with such a device should not find detection too difficult. One way is to search with a broad-bank re-

The internal homing device operates from inside the car, under the dashboard, or under the hood. It is used primarily when the length of time the automobile is to be under surveillance demands a more permanent installation.

ceiver, the same as for a bug in a premises. However, a physical check of the vehicle should do it, since hiding places are limited and the Bumper-Beeper must have an exposed aerial in order to function properly. If an initial inspection does not turn up the device, the vehicle should be hoisted on a grease rack and the underside examined. In addition to the inside of bumpers, the devices often are attached to the fuel tank and frame. In the case of devices connected to the battery, ignition switch or car antenna, inspection of the wiring may be necessary. One popular model feeds off the battery and is mounted under the dashboard.

Since most Bumper-Beepers are fairly expensive, owners are likely to attempt to retrieve them, providing an opportunity for identification.

In some cases the eavesdropper may not only want to follow the vehicle, he may wish to hear the conversations in it. A bug-transmitter will do him double duty, sending out a carrier that can be homed in on in addition to the voice modulation that can be heard by means of a receiver. The FBI termed its auto-bug the CAT, for concealed auto transmitter.

In searching for an auto-bug, the most likely spots are the interior recesses such as under the dashboard or behind upholstery fabric. Check under the hood for wires or foreign devices, such as antennae. As a further safeguard, do not park in open, unguarded areas. Vincent Gillen, the private detective who shadowed Ralph Nader for General Motors and also engages in debugging, recounted to *The New York Times Magazine:* "The president of a manufacturing firm on Madison (Ave.) found a bug in his desk and got so

scared that he discussed business only in his car. Then we found a magnet device shaped like a cigarette package under his dashboard. It transmitted conversations five blocks away." If a check is made with broadband receiving equipment in an attempt to intercept the transmission, the car's engine should be running, since some bugs are wired to the ignition system and transmit only when the switch is on.

If you have reserved a rental car from one of the car rental firms, it may be that federal agents or the police have placed a bug in the car in advance. Like the telephone company, these firms usually cooperate fully with law officers.

PART II

INDUSTRIAL ESPIONAGE

Industrial espionage, or IE as it is commonly known, has increasingly become a bleak fact of American industrial, commercial, and legal life. When multimillion dollar contracts hang in the balance, when trade and proprietary secrets spell a corner on the market, when strategy and future plans mean an edge on the competition, when a court case involving a large recovery is being planned, IE becomes a distinct possibility.

There is no way to determine the magnitude of the problem, since the attempts that come to light are probably just the tip of the iceberg. But the practice is widespread enough, actually or in the mind of potential victims, that the American Society for Industrial Security estimates there are close to 800,000 men involved in industrial security today. This represents a quantum leap from the 1950 estimate of 450,000, and is approximately double the manpower of the nation's state and local police forces.

Let us consider first the counterelectronic invasion phase of this effort. Since the IE game is played for much higher monetary stakes than normally encountered in other snooping, the re-

sources behind the eavesdropper are likely to be much greater. He will have more sophisticated gear, and probably is better qualified technically. This combination can be deadly unless met with equal resources. Some executives employ stopgap measures, such as equipping their security staff with full-band receivers and carrying compact field strength meters with them to conferences. But the best insurance – and it never can be 100 per cent – is to retain a firm specializing in electronic countermeasures and defense.

These firms are dotted around the country. In San Francisco there is Saber Laboratories, a division of the Fargo Company which markets police equipment. Saber bills itself as a "technical security support and countermeasure system." It offers bugged executives "information, knowledge, and training on setting up procedures for the protection of your company against the penetration by physical, mechanical, and electronic methods used by industrial espionage spies" plus "a complete set of scientific instruments to detect and/or jam clandestine eavesdropping devices, whether by telephone, miniature transmitters, miniature microphones, or other sonic eavesdropping devices." In its brochure, Saber points out that in the 1964 political campaign, both sides indulged in electronic snooping, and Saber leased countermeasure kits for the duration of the campaign.

Another defensive firm is John A. Kennedy & Associates of New York. Some who offer the service are accomplished buggers in their own right. Harold Lipset of San Francisco, who demonstrated the olive-in-the-martini bug before the Long subcommittee, provides electronic sweeps.

One firm's president held a press conference in July, 1967, at which he exhibited a number of bugs he said were uncovered. Among them were a bug with its antennae woven into a rug in the board room of a large rubber company, a voice-actuated recorder concealed in the hollowed-out encyclopedia in a manufacturer's office, and a tiny transmitter built into an ersatz cigar hidden in a humidor in a large drug company plant.

But as an article in *Machine World* for August 29, 1968, put it, "A word of caution about this hiring process. Unfortunately there are a number of unscrupulous private investigation firms around who offer this service and are not adverse to playing both sides of the espionage fence. It is always wise to check out the credentials of any agency carefully before hiring it for the sweep job. Otherwise, there is extra risk of a double agent moving in."

Another consideration is equipment. Paradoxically some of the nation's largest investigative firms, which offer "sweeps" as part of their service, have alloted all too little money to the purchase of equipment. Any firm representing itself to be proficient in this field should have an investment of between $5,000 and $12,000 in electronic gear. One of the finest pieces of equipment available is the Modular Bug Exterminator. This model has 12 plug-in modules that will sweep the spectrum from two KHz to two Gigahartz. It will detect wired, wireless, and has a "visual scanner" – an oscilloscope – that will show the wave forms. But it sells in the $9,000 range, which puts it out of reach of all but the most affluent debuggers. Thus, while there are cut-rate sweepers, anyone with the full range of equipment must charge in the

This attache case contains sophisticated equipment that sends and receives coded messages.

neighborhood of $500 and up a sweep because of his heavy investment.

The total problem of combating IE is a complex and costly enterprise, and is beyond the ken of this volume. A number of manuals and texts have been written on the subject, and several firms, notably Kennedy of New York, the Wackenhut Corp. of Miami and Dale Simpson & Associates of Dallas, have made a big business of the service. Unfortunately, most of these firms recommend polygraph examinations for employees, closed-circuit television monitors, and other techniques that are tantamount to invasion of privacy in the name of security. Some of these firms also supply undercover agents to go on the firm's payroll.

How the Industrial Spy Operates

The field of industrial spying opens up a brand-new profession for ambitious young men. In a U.S. Government Printing Office publication: *Invasions of Privacy: Hearings Before The Subcommittee On Administrative Practice And Procedure, etc.; Second Session Pursuant To S. Res 190, Part 5*, a report by a professional industrial espionage agent is most revealing. The period covered by the report is only three months, but note how much information can be obtained in such a short period of time.

(Report by David Terpstra).

Re: H. L. Moore Drug Exchange,
New Britain, Connecticut

7/14/65 This morning I had an interview at

the H. L. Moore Co., and I was well-received. I was told that he had no openings at the present but that he would let me know as soon as he had something for me. I told him that I had worked for Brunswig in San Jose, California for about 6 years and had just moved East because my family was settling here. Tomorrow I will bring him a telephone number, at which I can be reached.

At that time, I will also let him know that I got a job elsewhere in town but that I would still like to work in the drug field, because of background in it, and that I would still like to come to work for him as soon as he has an opening for me. I was hired by the Skinner Precision Instruments, Inc., at 95 Edgewood Avenue, New Britain. I will take a physical and start work there on Monday, July 19th. My hours there will be from 8 A.M. until 4:30 P.M., with a half-hour off for lunch, and I will work 5 days per week, and will be paid at the rate of $1.77 per hour. I was told that they pay on Fridays but hold back the first week so they have time to adjust their payroll. At Skinner, I used exactly the same background as I did at Moore. I will be living in a rooming house, the Glenn Main Hotel, which is only a ten-minute walk from Moore and 30 minutes, by bus, to Skinner.

7/19/65 Today I started work at the Skinner Company. As far as I can tell, they assemble electrical valves, the body of which is manufactured by Skinner, while other parts are done elsewhere. I do distribution work (similar to picking on a line) and I also pack orders. All of the material worked on here is exclusively for commercial systems using these valves.

7/20/65 through 7/30/65 – working at Skinner

Precision Instruments, Inc. I did not hear anything from the H. L. Moore Company yet.

7/31/65 Today I received a letter from H. L. Moore asking me to phone Mr. Moore to make an appointment with him for an interview.

8/2/65 I phoned Mr. Moore and had my interview with him. I was hired to start work at H. L. Moore Drug Exchange tomorrow, Tuesday, August 3rd, 1965.

8/3/65 I started to work for H. L. Moore at 8:30 A.M. My hours will be from 8:30 to 5:30 P.M., with an hour out for lunch, and my salary will be $1.75 per hour. This morning I was brought to Sam Moore (the brother of the other Moore who hired me) and he was to show me around. When he showed me the Receiving Department, which is in the cellar, 150 cases of Wyeth S.M.A. Liquid was being received, together with about 12 dozen Emko Refills, which did not appear on this invoice although they could have been on another. The invoice was from the Biddle Purchasing Co., 280 Broadway, New York, New York, and only showed 150 cases of the S.M.A. During the day, I spent most of my time checking orders which have to be sent out.

This is all broken-up shelf stock, however. All incoming shipments here are immediately stripped of all addresses, serial numbers, etc., and there is no other way of knowing where it comes from or where it goes, unless I will be able to check everything coming in, at the time it arrives. They don't seem to push the employees too much here and from what I saw so far, they all seem to get along well.

8/4/65 Today I was given the job of checking incoming shipments in the basement area.

1—We received a shipment of Marion Labs, Products, from Lenoco International Corp., 24 Stone Street, New York 4, New York, as follows:

Item	Amount per bottle	Total price	Invoice quantity	Quantity received
Anasorb	M	$ 96.00	2	2
Capre	200's	151.20	48	55
Do	500's	61.00	4	4
Capre-Flor	100's	113.40	36	40
Duotrate	500's	300.00	12	12
Do	M	570.00	12	3
Duotrate PB	M	693.00	12	13
Duotrate 45	100's	1,350.00	180	198
Do	M	1,800.00	30	33
Do	500's	580.00	18	20
Duotrate 45 PB	100's	1,050.00	120	132
Do	500's	693.00	18	20
Do	M	1,278.00	18	20
Furmasorb	100's	54.00	6	7
Oscal	100's	489.60	288	319
Do	500's	288.00	36	40
Do	M	1,080.00	72	78
Oscal-Forte	100's	162.00	72	79
Do	500's	114.00	12	14
Do	M	210.00	12	13
Oscalgesic	100's	374.40	144	159
Do	500's	138.00	12	14
Do	M	252.00	12	13
Osvim	500's	195.00	10	11
Pharagesic	100's	144.00	24	26
Zamitol No. 1	100's	79.20	24	27
Zamitol No. 2	100's	206.40	48	55
Zamitol No. 3	500's	76.50	2	2

This invoice mentioned 10% free goods and a total of 52% discount. The total price, net, of the invoice, which had been paid in cash was $7,167.60.

2—We also received a McNeil shipment, Invoice #72851, sent by the Kent Pharmaceutical Co., 8533 Everett Avenue, St. Louis, Missouri. This invoice read:

Item	Price per bottle	Total	Invoiced	Received
Butisol-Sodium, ¼ Gr.—M..	$ 8.79	$13,185.00	1,500	1,500
Butisol-Sodium, ½ Gr.—M..	11.40	17,100.00	1,500	1,500
Butibel—M	9.59	479.50	50	144
Syndrox—M	11.57	578.50	50	50
Butisol-Sodium, ¼ Gr.—5M	43.73	1,574.28	36	36
Butisol-Sodium, ½ Gr.—M..	57.81	2,081.16	36	36
Total		34,998.44		

The over-shipment on Butibel was not accounted for on the invoice and I don't know what they are doing on that, as far as payment is concerned. The whole invoice was termed "cash" and had been marked paid by the office.

Attached are a few labels I found on the floor, from previous shipments, and where possible I have noted the merchandise shipped:

#1—From: Standard Drug, Detroit, Michigan, "500's Trate r (ripped label)" addressed to: H. L. Moore Drug Exchange.

#2—From: Marion Laboratories, Inc., P.O. Box 963, Kansas City, Missouri, addressed to: A. D. Pier Terminal, 75 Beach Street, New York, N. Y.

#3—From: Standard Drug. 1354 Lafayette Ave., Detroit, Michigan, addressed to: H. L. Moore Drug Exchange – containing *Warner-Chilcott* merchandise.

#4—From: D. A. Rosow, Inc., 184 Fenn Road, Newington, Connecticut. #19476.

#5—From: Brown Wholesale Drug Co., P.O. Box #2130, Newark 1, New Jersey, addressed to: H. L. Moore Drug Exchange. #47429.

As reported, the addresses are immediately removed from the cartons and thrown into a metal drum, and they are burned in this drum, at the back of the parking lot, at the end of the day. I

still haven't seen any S.K.F. merchandise come in, but I understand that each time it does, it totals about $60,000.00. I also heard they ship out approximately 80 to 90 orders per day. Jerry Rome told me today that Mr. Moore is raising me from $1.75 to $2.00 per hour because he felt it was warranted.

8/5/65 I was supposed, to start order-filling today, so Mr. Jerry Rome said he was going to give me a little indoctrination. He started out by telling me never to mention any names because the suppliers, as I would have already understood, did not send their merchandise direct (meaning from the manufacturers), but from other sources, much cheaper. He said, "This is slightly illegal and, if known, would run us right out of business." I told him I would remember that. He then said they were glad to have me here and there was no limit as to how far I could go with them (providing I do as I was asked, meaning the above). A Lilly shipment was delivered today, coming from Webster Drug, 546 North Avenue, Long Island City. This man was still there after lunch and I learned that he handles the transactions between Webster and Moore. I don't know if he is the boss there or not, but he looked too well-dressed, etc. to be a salesman. There were about 30 cases of Lilly involved, all with Commons Brothers stamped on them. There was also a small shipment with "Endo Labs." on it, but this contained a lot of assorted merchandise. I heard Jerry say that there is U.S. Vitamins merchandise coming in one of these days, also from Webster.

Enclosed are two labels I found on the floor today:

#1—From: Ayerst Laboratories, 245 Paterson Avenue, Little Falls, New Jersey, addressed to: David A. Rosow, Inc., 184 Fenn Road, Newington, Conn. containing: *About 6 Repacks of Ayerst.*

#2—From, or to: Millbrook Pharmacy, 230 Brook Avenue, New York, New York, containing: either *S.K.F. or Robins.*

I believe I am very well-trusted by everyone here and they seem to like me personally as well. I will be an order-filler from now on, but I also may do some checking as well.

8/6/65 They had me filling orders for the greater part of the day. A lot of shipments came in today, but I only checked one. It was a Winthrop shipment and it came from M. Sobel, 507-609 East 165th Street, New York City. I don't know if this is a wholesale druggist or not, but nothing else was marked on the shipment. I found some labels from incoming Parcel Post shipments—and these are enclosed:

#1—From: W. C. Cable, 43 Beaver Place or Street, Brooklyn 6, New York, addressed to H. L. Moore Drug Co.

#2—From: Lisa Monet, Inc., 89 Tec Street, Hicksville, L.I., N.Y. 11801, addressed to H. L. Moore Drug Exchange.

#3—From: Biddle Purchasing Co., 280 Broadway, New York, New York, addressed to H. L. Moore Drug Exchange.

I do not know what those packages contained. The following Lilly items are always being split-up and sold in packages of 500 (10 such plastic

bags make up the 5,000 but they are not supposed to be broken-up): Accidulin, Amytal 3 Grain, Seconal Sodium ¾ Grain, Seconal Sodium 1½ Grain, Trinsicon-M, and Trinsicon #2-Lilly. According to Mr. Rome, this system gives them a $2.00 per bag of 500 extra profit, and he said the customers don't mind this. I also saw an invoice for a shipment containing 300 bottles of Pro-Duosterone 24's, which were sent by Berger Consolidators, 217-07 74th Avenue, Bayside, New York. The interesting part of this was that on the bottom of the invoice the following was typed: "This shipment not to be resold in the Continental U.S.A.—Strictly for export to Liberia."

According to Sam Moore, a lot of their shipments are exactly that (meaning for export) and that's the reason for their never knowing how much they will be able to get when they order. I counted the Azulfadine Tablets to be reordered and the figure of stock on hand was approximately: 800-100's, 96-500's, and 120-1000's. He was going to order about the same, but he said that if he could get 2000 100's now for a good price, he would only buy that much. When we run short or out of an item, it is never backordered or marked to follow, unless the amount is such that it warrants an extra shipment. All orders apparently ranged between $500 and $2,000 and I have seldom seen one below $500. We still haven't been really rushed with work, though.

8/9/65 This was a very busy day here, which is usual for a Monday. I spent the whole day working on orders and could only glance at the incoming shipments. A large shipment of Merrell Company merchandise came in, but it came directly from the factory. An Ortho shipment came

in earlier, without me seeing it, and this either came from or through Webster Drug. A lot of small stuff also came in, but I wasn't able to determine its origin as the labels had already been cut off. All of the cosmetics orders I've seen so far have come directly from the manufacturers.

8/10/65 A lot of shipments came in again today, mostly cosmetics, and they came from the manufacturers who produce them. There was also a Stuart Labs. shipment which consisted of 200 cases and came from David A. Rosow, Inc., 184 Fenn Road, Newington, Connecticut, P.O. No. 07426465. A Searle shipment also came in, but I don't know how many cases were involved in that, because of the repacks, but while Sam Moore was checking it, I saw that the total amount paid for it exceeded $12,700. This consisted of mainly Enovid and Enovid-E, and this was sent by Webster Drug Co., 75 Monroe Street, New Britain, Connecticut. I have no way of knowing if this is the same Webster, using another address, that we received other goods from in the past.

8/11/65 Considering that this was a Wednesday, we had a busy day. Until lunch, I worked on nothing but filling orders, and then, after lunch, I checked the same orders. A Johnson & Johnson shipment came in, and the label is enclosed, reading:

> From: En Bee Drug Co., 31 Wilson St., New Britain, Conn. 06051, customer order No. 2169, B/L No. 338710, marked "No delays. Accept after 1 P.M." Associated–08/06/.

I don't know how large this shipment actually

was, but it was easily 200 cases. A Bristol shipment also came in, sent by:

From: Maddi Drug Co., 345 West Jefferson Street, Syracuse, New York.

I was putting up some S.F.K. stock this afternoon, and a few labels were still on a few cases; that is, pieces of labels were on them. I am quite positive that this shipment had come through Webster Drug, here in Newington. We still haven't received any S.K.F. merchandise, though, since I have been working here.

8/12/65 Because we again weren't very busy today, I spent most of the afternoon stocking shelves, preparing for the rush on Monday. About 600 cases of Johnson & Johnson came in, with the sender marked as:

From: Abnee Drug Co., 574 Monroe Street, New Britain, Conn. (I may be wrong on this street address, but the address was definitely the same as the Webster Drug address).

We also got in a cosmetics shipment and the label is enclosed, reading:

From: Crestwood, Pa., Mt. Top, Pa., Inv. No. 33625, to: Axelrod's Phcy. (on 25), 37 Broad St., New Britain, Conn.

Tomorrow we are supposed to receive a shipment of Geigy Products, through Rosow. We are sending them a shipment of patent medicines and, according to Sam, they will bring us the Geigy when they pick this up.

8/13/65 Today, through Webster, we got in Mead Johnson and McNeil. The McNeil merchandise was the balance of what was ordered on the invoice I copied and sent to the office previously. According to Sam, this order totaled somewhere around $10,000. The odd part of this is that it came through Webster, but I cut off it the enclosed label reading:

From: D. A. Rosow, Inc., 184 Fenn Road, Newington, Conn.

Enclosed also is a label from a shipment of 200 cases of Stuart Products reading:

David A. Rosow, Inc., 184 Fenn Road, Newington, Conn. P.O. No. 07 & 26 & 6-?5.

Also enclosed are two labels that I found thrown out in the cellar, which prove that S.K.F. merchandise came in from Webster Drug. One label came on a case of Stelazine-R, 2 Mg., 500's. The other looks as though it came from the same kind of case, but I can't make out the product name, but that is also 2 Mg.

Enclosed also is a small label. I don't know what this contained, but the enclosed label reads:

"Ship to": #662422: Worcester Medical Supply, 212 Front Street, Worcester, Mass.

For a complete rundown of the people working here, please note the following:

Mr. H. L. Moore: He's President of the Company, but he works on orders every day, the same

as any other picker here does.

Sam Moore: Brother of H. L. Moore. He does the buying and inventory, and he also checks in merchandise and picks orders alongside of me.

Jerry Rome: He is apparently the "power" in the Company. He does all the hiring and firing, makes decisions on accounts, decides what and when to buy and is the "know-how" of the Company.

Mr. Goldfarb: He is the Office Manager, runs the office and dispatches the orders to the warehouse. He also invoices them after the orders are picked.

Ann Herson: She runs the Tab. Room.

Steve Herson: He's Ann's son. He is an order-picker in the Rx Section and usually works along with Sam Moore. He is "Sam's boy" and his confidant.

Grant: Is an order-picker in Pharmaceuticals. He is hard of hearing and is a slow worker.

Besides myself, there is also a girl working here, who is now on vacation and that is the complete rundown of the Rx Room personnel.

Abraham Burkowitz: He handles shipping and general duties in the shipping room.

Les or Lex: He's the foreman, more or less, in packing and shipping.

Bob: Is a packer.

David: Is also a packer.

A Negro Boy: He also works on packing, but I don't yet know his name.

Cosmetics Room: There are 2 girls and a man working there. The man is in charge of buying cosmetics and over-the-counter medicines, all non-Rx. I don't know their names yet.

O.T.C. Room: There is 1 man and a woman

working here, but I don't yet know their names either.

I mentioned three sections here, which are really three buildings that are connected. The orders are started in Cosmetics, then go to O.T.C., and to Rx last, after which they are checked item by item against the tabulated invoice. There are three more girls working in the office, who do the payroll and mailing and whatever else has to be done there. Jerry Rome seems to have "final say" in all these departments.

8/16/65 This was a very, very busy day here and I couldn't get much checking done. Webster came in with merchandise from assorted companies. I don't know the amounts or exactly which companies were involved, but Lilly and Warner Chilcott were both included. A very big shipment of Emko Products also came in, around 60 cases of it, but a lot of repacks. I didn't even see that unpacked, but it was sent in by Lisa Monet, Inc., 89 Tec Street, Hicksville, Long Island. I expect an S.K.F. shipment to come in any day now, because the shelves in overstock are fast being emptied of their items.

8/17/65 Not even one shipment came in today and since we also had very few orders, we had an easy day. We finally wound-up stocking shelves to "kill time." Steve Herson is going on his vacation, starting Thursday. After that, he will only be working part-time here because he is returning to school. Today I learned that Mr. Wolfe is the man who is in charge of cosmetics and over-the-counter merchandise. He does all the buying for those departments and is directly "under" Mr. Moore and Jerry Rome. The fellow

who works the orders in the over-the-counter room is Aldo Berti. Everything else was routine and I learned nothing from the conversations I had.

8/18/65 I was ill and didn't work today.

8/19/65 This was a rather slow day here. We had only one shipment come in, containing over-the-counter items and cosmetics. Enclosed is the label, which reads:

> From: Leonard Wholesale Drug Co., 1050 Sherman Avenue, Elizabeth, New Jersey.
>
> For: Moore Drug Exchange, Inc. (36551), 610 Arch Street, New Britain, Conn. (Parcel Post).

Because Steve is on his vacation, I had to pull cards for shelf stock. I told Sam that we were particularly low on the following big, fast-moving lines: S.K.F., Robins, and Warner-Chilcott. He replied that S.K.F. is on its way, as well as Warner-Chilcott, and that he had just placed a very big order for Robins. He complained to me that the first two lines would most probably come in together and jam-up the place for a week, because of the sizes of those shipments. I am fairly well convinced that their last S.K.F. shipment came through Webster Drug and that their next one will also. I haven't yet seen the order around, but I will at least get the amount of the order, if I am not able to itemize it.

8/20/65 On Monday, we will receive an S.K.F. shipment of approximately 290 cases. Burkowitz mentioned it to me today and said he had called for it. This is coming from somewhere in Minne-

sota and through Webster Drug. The shipments we got in today came directly from the manufacturers involved and labels were not cut off those. They only remove such labels when the merchandise comes through "special companies."

8/23/65 This was an extremely busy day here; in fact, we only got about halfway through with today's orders. The following shipments came in from Webster: Merck Sharp & Dohme, Massengill, Lilly, Mead Johnson, and Geigy. I could learn nothing about them, as to size, original shipping dates, or costs. These, apparently, consisted of fill-ins, rather than being full orders. Smith, Kline & French Products came in, but it was too late to unload it today, so it will still be there tomorrow. This consisted of 290 cases, with a total invoice price of $76,000, according to Sam Moore. This is from Webster, but I will try to learn who made the original shipment to Webster. We also got a shipment of Robins merchandise today, from Webster, worth $14,000. However, all labels had already been cut off that shipment and I could learn nothing more about where it had come from. The next big shipment expected here is Warner-Chilcott.

8/24/65 Although I tried my best to get hold of some of the labels from the S.K.F. shipment, I couldn't do so safely, so I let it go for the moment, and I hope to get at least one tomorrow morning, before they are burned. Lilly came with it, and Hoffmann-La Roche, about 30 cases of the Lilly and approximately 50 La Roche. I didn't get a chance to get near those at all, and I made this count quickly from a distance. Shipments of so many other companies also came in this afternoon that I had no chance to see what and from

where, but I will check those out when I have an opportunity. Incidentally, the Roche shipment did not come in from Webster, it came from Dept. Sales Co., 31 Wilson Street, New Britain, Connecticut (Note: List Book indicates Drug Sales Co. buyer is A. Rosen, for G. E. Madison Stores, Inc. (Discount Stores) at 750 Queen Street, Southington, Connecticut.)

I am now fairly sure that Moore continually orders from the same suppliers because Sam Moore told me this morning that he likes to buy his merchandise from the one place, rather than have three or four different suppliers for the same company's products. Since things are going so well for me here and I have definitely gained Sam Moore's confidence, as well as others', I'm only securing labels when it is safe and I am unobserved, so there will be no chance of anyone catching me at it. Incidentally, the Lilly and S.K.F. shipments were delivered by Spector-Mid-State Trucking.

8/25/65 A lot happened here today. First, 189 cases of Smith Kline & French merchandise came in (not 150 as I stated on the telephone earlier), which "Burky" (Burkowitz) said was worth $39,000. It came in during the coffee break, so I asked him if Webster had finally "come across" with the rest of the S.K.F. stuff. He said no, that this was from somewhere else, and he added, "Can you imagine, a mere 150 cases amounting to an invoice price of $39,000?" (This is where I got 150 from). He didn't say where it came from, and there were no addresses on the cases, they looked like they came straight from the Smith Kline & French Warehouse. If possible, I'll try to learn more about that. I got one of the address labels

from the S.K.F. shipment, but it only states that it was shipped from Webster Drug, Inc., New Rochelle, New York, to Webster Drug, Inc., 75 Monroe Street, New Britain, Connecticut. On most of the shipments we got in yesterday, the original address labels had been cut off before the Webster labels were applied to them. Enclosed is a label from the Hoffman-LaRoche that came in, from Department Sales Co., 31 Wilson Street, New Britain, Conn., 80173.

The 400 cases of Warner-Chilcott came in via Rosow. This seems to be a tricky deal – although I was checking-in the Warner-Chilcott, I saw that there were no prices on the order. When Sam joined me a little later, I commented that all I had was the bulk of Warner-Chilcott, and hardly any of the prescription items we really are short on. He explained this as follows: He orders the bulk or over-the-counter items from Rosow because it saves him a lot on freight, as the rest of Warner-Chilcott comes from Minneapolis, Minnesota. He said he did that with most companies, that if expensive enough and not too big, he will order from Minneapolis. Otherwise, he said, the bulk will come through local suppliers. Sam likes to talk about how well he does the buying, but Jerry Rome is doing these orders and Sam only warns Jerry when it is time to order more stock. From what he's said so far, it seems it probably all comes from the same place, but I'll try to learn more about this when Warner-Chilcott comes in again. Enclosed is a part of the carton, indicating that Warner-Chilcott was addressed to D. A. Rosow, Inc., 184 Fenn Road, Newington, Conn. (marked 22277-407). Enclosed also is part of the tape I soaked off another label (also en-

closed) reading: McKesson & Robbins, Inc., 285 Newfield Avenue, West Hartford, Conn. (#583-45). This was on 25 cases of Burroughs Wellcome Empirin Compound, 100's.

8/26/65 Nothing much happened here today. The bulk of Schering came in today, 108 cases of it, mostly the non-prescription items. These came in direct. However, the most important part of Schering comes from an indirect source. I have been trying to learn more about Smith Kline & French, but have come up with nothing more on that yet. I learned that the names of the two girls in the Cosmetics Room are Betty and Florence, and the girl in the over-the-counter area is Pauline. The two girls in prescriptions are Mae, who works beside me in the aisle, and Loretta who works with Sam while Steve is away. There is another fellow who works mostly on packing and he is Elliot. Bob is leaving next week, on Friday, to return to school.

8/27/65 We got a lot of mixed shipments in from Webster today, brought in by the man with the Cadillac. I learned that he is Hyman Boxer, and the license plate of his 1965 Cadillac is N.Y. 80-HB. He brought in merchandise from the following companies: Searle, Lilly, and Hoffman-La Roche, but these were all just fill-in orders. Besides Webster, we got in the following: Wallace Labs. merchandise, from The Biddle Purchasing Co., National – direct, Purdue Frederick Co. – direct, Riker – direct. We also got in Strasenburgh, but I don't know who sent it. But, it might have been Webster, since it came in while he was there, although it had already been unpacked before I had a chance to check the label. The same

thing goes for the Wampole Labs. merchandise also.

8/30/65 We were so busy here today that we only finished filling about half the orders. Webster Drug delivered a lot of merchandise that was short on the shelves, including Searle, U.S. Vitamin and, as usual, Lilly. Also about 30 cases of Sandoz and about 10 cases of Roche, and these all had the yellow Webster labels on them. There were also 3 repacks on Merck Sharp & Dohme, but I didn't see any labels on those. We also got in a little Geigy merchandise, but that came direct. I spent the morning filling orders and then checked during the afternoon. We had a very high rate of mistakes today, mainly made by Grant and Mr. Moore. Whenever Mr. Moore does the picking, his mind seems to work faster than his hands, so he forgets to pick half the orders called for.

8/31/65 We had another very heavy day, and I had to spend most of my time checking orders. D. A. Rosow brought in 102 cases of Smith Kline & French, most of which were unlabeled. However, I didn't get a chance to get one of those labels, but I will try to do so tomorrow. This shipment of 102 cases was delivered by the Rosow truck. We also got in Merrell and White Laboratories merchandise, but those came in direct. Mr. Boxer came in with 50 cases of Maalox Liquid and 7 repacks which bore only the single grease-penciled name "Bergmeyer." This was brought in by the Adley Ex-Press Co., but there was no further indication of its origin. A full shipment of approximately 100 cases (I don't know the exact amount) of Dorsey Labs. merchandise came in. I don't know for sure where this came from, but

my guess would be Webster Drug, since I saw their labels lying in the vicinity of this merchandise, where I had not seen any labels before the delivery was made. I'll try to learn something more definite on this also.

9/1/65 Today I didn't do much else, but stock and check in merchandise, because that tabulator broke down and invoices we use to check the orders didn't come out to us until about 4 P.M. The first thing I did today was put away the Smith Kline & French mechandise and, in the process, I found some pieces from these cartons which are enclosed, and which are:

#1—a piece of one carton that contained S.K.F. merchandise, with the red lettering, "D. A. Rosow, Inc., 184 Fenn Rd., Newington, Conn." on it (no other printing or lettering on this piece).

#2—a piece of another carton that contained S.K.F. merchandise, with larger red lettering, reading: "D. A. Roson, 184 Fenn Road, Newington, Conn." (note the incorrect spelling of Rosow's name). On this, there is also stamped or stenciled the numbers "838."

#3—a piece of another carton that contained S.K.F. Stelazine, 2 Mg., 500's, reading: "ineR—mg. Lot No. 2624796—D. A. Roson, 184 Fenn Road, Newington, Conn." (note incorrect spelling of Rosow on this also).

I then finished stocking some of the McNeil merchandise received in the $34,998 shipment. The items I worked with, among others, were Bu-

tisol Sodium, ¼ and ½ Grain, 1000's, ¼ and ½ Grain, 5000's, Butibel 1000's and Syndrox 1000's. These items are now being offered at a special price, 25% off. Sam Moore explained that's because he had bought these at the old price, but since then prices on most McNeil items have been increased. These items, along with some Lilly items, are listed on the specials order-insert sheets we send with orders, and I'll try to get a copy of that when they are left lying around again. These inserts are changed about every week, or they can come out with new ones any day, depending upon what they get in at a good price. The items we got in the second McNeil shipment are not on special. We also got in 16 dozen Mead Johnson Oracon Tablets 21's, repacked, but I don't know who from.

We also received Wallace merchandise: 12 dozen Capla 100's, 60 dozen Miltown-400 100's, 24 dozen Soma-350 50's, 12 dozen Miltrate-200 100's, 9 dozen Metrospan-400 100's, and 24 dozen Deprol 100's. This came from Lisa Monet, Inc., 89 Tec Street, Hicksville, L.I., N.Y. 11801 – addressed to H. L. Moore Drug Exchange, 610 Arch Street, New Britain, Conn. – and two of these labels and parts of cartons are attached.

We also received from Lisa Monet today: 13 cases (gross) Ortho-Novum, 2 Mg., 20's, dial pack – 2 dozen Searle Enovid 5 Mg. 100's, 2 dozen Searle Pro-Bathine, Plain, 500's, 15 Mg. – 2 dozen Searle Floraquin Vag. Tablets, and 6 dozen of a new Lilly items – Aventyl 25 Mg., 1000's.

9/2/65 Enclosed are two portions from the 16 cases of Mead Johnson Oracon that came in yesterday, both bearing the D. A. Rosow name and his Newington address. Attached also is a

sheet of the specials being offered on Lilly merchandise, on which I have marked the items being sold in plastic bags because they come from bags of 5,000 that were broken-up. These are now being offered by Moore up to 25% off. On the back of the second Lilly specials sheet, offering nitroglycerin items (with 10 and 25% discounts), are Emko Kits and Refills, listing them at 12 to 15% off.

We no longer have the specials on McNeil Butisol Sodium. No shipments of any consequence came in today, but Sam took inventory on Smith, Kline & French, so they are going to place quite an order for that, and soon. Also enclosed are specials sheets covering Binky Products, Clairol, Poser merchandise, Kodak Films, Dr. West Toothbrushes, Breck, Hask, Ozone's Stephens, VO-5, and Karena Hair Care Products. The other side of this last sheet offers specials on general merchandise, such as: Meprobamate, Prednisolone, Pentobarbital, etc. Also enclosed is a slip being put in with all orders, reading:

> "You'll profit – we'll profit – and your customers can profit . . .
>
> "We're always on the lookout for new sources of all types of drug store merchandise . . . if you come across a good deal that you think we may be interested in . . . let us know.
>
> "We are also interested in buying agency lines of cosmetics. If you can supply us please jot down the information below and we'll follow through. Thank you."

9/3/65 Today we got in a shipment of Ciba, but it came direct. Rosow also came in with a

fill-in shipment on Geigy, Searle and Lilly merchandise. The Lilly consisted of 14 cases of 5,000's Seconal Sodium, 1½ Gr. These are being broken-up and put into bags of 500's for our shelf stock. Biddle also sent in 36 Pro-Banthine 15 Mg. 500's, and 36 Pro-Banthine with Phenobarbital, 500's. Lisa Monet also sent us 3 more cases of Ortho-Novum 20's, 2 Mg. Sam Moore, Jerry Rome and Mr. Goldfarb were very upset this afternoon because an auditor came in to check their books. From what I could hear, the trouble was about invoice numbering and invoices covering interstate selling of merchandise. I couldn't overhear any more about this today.

Enclosed are some specials sheets which are being enclosed in orders now. The enclosed outer-page only of the Summer-End Specials (which is a booklet) features special offers and discounts on: Abbott, Ayerst, Breon, Bristol Labs., Chanel, Inc., Chesebrough-Pond's Wind Song, Christian Dior, Ciba, Cigone Sortilege items, Cole Chemical, Coty, Dana, D'Orsay, Dorsey Labs., Emko, Flint Eaton & Co., Geigy, Houbigant, Lakeside Labs., Lanvin, Lederle, Lentheric, Marion Labs., Max Factor, McNeil Labs., Mead Johnson, Merck Sharp & Dohme, The William S. Merrell Co., Monico, Ortho, Parke Davis, Pharmacia Labs., Pitman-Moore Co., Purdue Frederick, Raphael, Reed & Carnrick, Revlon, Roerig, Schering, Schiaparelli, Searle, Shulton, Squibb, U.S. Vitamin, Walker Labs., White Labs., Winthrop, Wyeth, and Wynn Pharmacal Corp. Enclosed is another specials sheet, covering close-outs and overstock specials — this includes the same companies named in the Summer Special, plus S.K.F., Charles Antell, Remington Monarch Typewrit-

ers, Elizabeth Arden, Hattie Carnegie, Carven, Dorothy Gray, and others. A third specials sheet is also enclosed, offering Lilly items at up to 25% off, and Clairol at list (wholesale) less 15%. Also enclosed are two bills, written up by Jerry Rome, to cover my personal order. He told me to destroy these bills when I'm finished with them because I can "cause a lot of trouble with them."

9/6/65 Labor Day – we didn't work.

9/7/65 We had a very busy day here and only got half finished with the orders. Rosow came in with a mixed shipment, but mostly Geigy, and I'll see if I can learn or see which items were involved tomorrow. In there also were 4 cases of Lilly Trinsicon 5000's and 2 dozen Isolone Chewables, together with some mixed Mead Johnson merchandise. I didn't get much time to speak with the others here and learned nothing new from what they did say.

9/8/65 I spent this entire day checking, because there were hardly any orders to work and a lot were left over and unchecked from yesterday. I left at 3 P.M. today. Sam told me that instead of losing the two hours pay, I could come in an hour earlier tomorrow and make up for it. They are very considerate of their employees here and, once in a while, they even ask whether my parents got their visas and will be here soon. I'm using the delay in getting the visas as my excuse for not having brought them to this country yet. We got in some Parke Davis merchandise, from Dept. Sales Co., but I don't know how large it was. We also got in a Johnson & Johnson shipment, from En-Bee Drug. Since we don't carry much J. & J., the shipment wasn't as large as it should be for such a large manufacturer. We

also got in a full shipment of Searle, but I don't know where it came from yet. The same thing also goes for Schering. These came in repack boxes but I didn't have a chance to look if there are addresses on them. This was the type box that Rosow uses, but the only name I saw on there was H. L. Moore. This J. & J. shipment included Micrin and Band-Aids.

9/9/65 This was a slow day, except for the incoming merchandise. A full shipment of Searle merchandise came in from Standard Drug, Detroit. I don't know exactly how large the shipment was, but it did cover their full line. Mr. Boxer also came in again today and unloaded from his Cadillac the full line of Mead Johnson Products and about 30 cases of Lilly merchandise. This was all stamped "Commons Brothers." Sam Moore checked this all in, so I didn't get a chance to look at what items were involved. However, most of the Lilly items we had up here, and definitely all delivered by Webster, are marked "Commons Bros." Sam Moore also ordered some fill-ins on McNeil merchandise from Rosow tonight, to carry us over on out-of-stock items. One of the items involved was Butisol Sodium, of which we didn't have a single bottle left in stock, on the ½ Grain.

Today also, Sam Moore introduced me to Mr. Boxer. He asked me to take inventory on Warner-Chilcott and Robins, saying it would take a long time to get. He explained this: "We order from this gentleman here (meaning Mr. Boxer). He sends our order to Minneapolis, they fill it and send it to Webster Drug, which is here. After that, we pay Boxer who, in turn, pays Minneapolis." He told me all this, but he didn't mention any

names in connection with Minneapolis. On these two lines, we get everything from Minneapolis, except for some bulk items or fill-in orders. I overheard Mr. Boxer say, "Your Geigy order was only $5,700," and he must have meant the Webster Drug shipment that came in quite a few days ago, because the Geigy merchandise that was delivered on the 7th was much more than $5,700. Incidentally, on the Robert Wood Johnson shipment we got in yesterday, I couldn't get any of the labels, but the label I saw read only "En-Bee Drug," with no street address for En-Bee, and then simply read "Deliver to: H. L. Moore Drug Exchange, 75 Monroe Street, New Britain, Conn."

Today Sam Moore also told me that on Lilly Alizone Pulvules, 100's, they got them from Webster Drug who got a 12% discount from Commons, that he gives Moore 6% and Moore makes 5% clear profit on the 250 Mg. 100's. Sam also told me that he ordered the full McNeil line but it won't be in until sometime next month. Betty from the Cosmetics Department told me that Dept. Sales Co. supplies Moore with all the cosmetics, with a lot of free goods. She also said that last Christmas Moore got 800 cases of a particular Faberge Cologne as free goods, that they erased the "sample" marking on them and are now selling it for $4.00 a piece.

9/10/65 This was a very quiet day here, so we worked mostly on stock and preparing ourselves for Monday. We got in one shipment from Lisa Monet, Inc., containing assorted stock we were out of. Most of this was Merck Sharp & Dohme. A little was also Mead Johnson Oracon Tablets, which had been omitted on the large

Mead Johnson order we got in the other day. They also sent us two or three Lilly items that we weren't able to get in the Lilly order delivered recently. Everything else was quiet here today.

9/14/65 We didn't have too many orders for a Monday and the bosses seemed somewhat frustrated over this. There are a lot of McNeil, Mead Johnson, and Lilly items that we can't seem to get enough of and, consequently, have to short. Butiserperide 50 Mg. 50's is one of them; we have been out of it for over a week, and it's one of the fastest-moving McNeil items. Ilosone Pulvules 250 Mg. 100's, made by Lilly is another one. Also, on Oracon Tablets, I've had to short at least 12 dozen because they are unavailable.

Rosow today delivered a Roche shipment. I counted 32 cases and 4 repacks of it, but I don't know which items were involved and how many pieces of each came in, nor do I know the total dollar amount of the covering invoice. However, it was a full shipment. On Roche, our only good-movers are the 500's and 1000's, and we don't carry too much in the 50's size. Lakeside and Alcon merchandise also came in, but both were direct shipments.

9/14/65 Today we had many more orders than we usually have on Tuesdays, so we were all kept very busy throughout the day. We got in 32 cases of Smith Kline & French, but I don't know where it came from and there were no markings of any kind on these cases. Sam Moore checked that shipment in himself. We also got in the full line of Lilly Products that we carry, and this came from Rosow, 60 cases in all. The full line of Eaton Labs merchandise also came in, also from Rosow. We got in a little Merrell mer-

chandise too, but I think that came direct from Merrell because the cases were factory-sealed and the Moore address was on them. Rosow also sent us a Geigy fill-in order, 36 dozen cases that I counted on that.

Mr. Moore today changed around our system, as far as ordering new stock is concerned. Until now, when we were running out of an item, we were supposed to note it on a blackboard, so Sam would see it and order it. However, a few weeks ago, I suggested to Mr. Moore that instead of doing that, we should pull a card when we run low on a particular item, so we can order more stock of it before we run completely out of it. We will now follow that plan.

9/15/65 This wasn't a very busy day here otherwise, but we got in a lot of merchandise, so it was a confusing one. Too many things came in today for me to give exact figures on. While we got only two deliveries, several companies were involved. Full shipments, meaning the entire lines, were received through Sobel, and they were Lloyd Labs., Dome Chemicals and Ives-Cameron. Both Lloyd and Ives-Cameron were immediately reordered because the shipments we received were too limited, but I don't know if they were reordered through Sobel or not. Fill-in shipments were also received through Lisa Monet and were the following: Lilly, Searle, Ortho, Winthrop, and Warner-Chilcott. There wasn't much of each one, except for Winthrop. We don't carry the Winthrop Line in too great quantities, but this looked like it could have been the whole line. National came in also, but direct, and so did Sherman Labs. Poythress also came in, but I couldn't determine where from because it was

received while I was out for lunch.

Mr. Moore and Jerry Rome were talking today about a cosmetics line (I don't know which one) where something must have been wrong, as I heard part of Jerry's sentence, "I don't care if you keep or expand that line. It is your neck, not mine, that gets in a jam with this." Later, I heard Mr. Moore outside on the telephone, presumably talking about this, cancelling a proposal for a sale on this certain thing. Jerry seems to be the one most aware of and concerned with the legalities involving sales and the like.

9/16/65 Since the orders were very light today, we spent a lot of time stocking shelves. At about 10 A.M., a shipment of Emko Deals came in, 8 cases, each about a cubic yard in dimension. The labels were cut off those as fast as they came in because, I assume, they were intended for export. I couldn't get hold of any labels showing names and addresses, but enclosed is a portion of the paper on one case, reading: "Glass, Handle With Care, Vidrio, Maneje Con Cuidado." According to Sam Moore, $56,000 worth of S.K.F. is expected tomorrow, and he said he got the confirmation on it today.

Hyman Boxer was here again today and since Sam was speaking to him, I believe it will be from the usual source. When I had to fill the shelves, Sam told me that when I came to Wallace, I was to take this stock from a place separate from where Wallace is usually kept. He said he had gotten $60,000 worth of Wallace last night, which was for export and has special codings and markings on it, so he wants to get rid of that first. The labels on this were already gone but, based on the cut of the label, I believe it may have come with

the Rosow label on it. I have no proof of that, of course, but I'll see if I can't find one somewhere that wasn't entirely cut off. We also received an enormous amount of cosmetics today, but I have no information on that at all. However, this numbered in the hundreds of cases and involved assorted manufacturers.

9/17/65 We weren't busy today, so we spent a lot of time on stocking the shelves and cleaning-up in general. Mr. Moore asked me if I would like to build some shelving for them downstairs, either during the week or maybe next Saturday morning. He said he would rather have me do it than an outside carpenter because, if they had an outside man, one of them would have to come in, which wouldn't be necessary if I did it. I fully agreed to do that job on Saturday morning, and they immediately ordered the lumber.

We didn't get any shipments today, not even the Smith Kline & French that we had expected. In my September 15th report, the day we got in assorted merchandise from Lisa Monet, Inc., I forgot to add that some Pfizer merchandise also came in from Lisa Monet, in repack cases, not full cases. A few days ago, we also got in a small Pfizer shipment from Rosow, also repacks. Moore doesn't carry too much of Pfizer, but he does have some; however, I have never seen any full cases of it come in, it was always in repacked cases.

9/20/65 Today we had so many orders to fill that although we worked on them all day, we couldn't finish and will be working them tomorrow also. The first thing this morning, Rosow came in with Stuart merchandise, 246 cases. Then we got in 70 cases of Burroughs Wellcome, from McKesson & Robbins, most of which was bulk,

such as Empirin Compound Tablets, etc. We also got in direct shipments from National, Lakeside, and Merrell. There was very little of the Merrell, only items we were low on. The Smith Kline & French shipment we expected has been delayed, and I understand it won't come in until Tuesday or Wednesday.

9/21/65 Although the individual orders to be filled today weren't too heavy, we had quite a few, so we had a very busy day. Today Spector Mid-States Trucking Co. delivered the Smith Kline & French shipment, addressed to Webster Drug Co. I saw the invoice, and it called for 289 cases, stating it was sent from the Webster Drug Co., Minneapolis, Minnesota (no street address), to Webster Drug Co. here on Monroe Street. Before the Webster label was applied, though, another label had been cut out. The total invoice price was $56,000 and some cents.

They also brought in a Searle shipment, on which the total price was $8,334 and some cents. In addition to those two, Spector also delivered an Ortho shipment, on which the price was shown as $15,000. However, I saw the Ortho shipment and I would say it was only for about $5,000. However, it may be that there is more coming in on that. A lot of Lentheric items were also included in this shipment (cosmetics), but I wasn't able to get figures or any other details on that today.

9/22/65 This was a slow day here, but we had a lot of stock to put away, especially with what we got in yesterday. Today all we got in was 44 cases of Warner-Chilcott, brought in by Rosow. This consisted mainly of Peritrate SA, 80 Mg. in 500's, which we had run out of. According to Jerry Rome, since we have been sending out the specials

sheets, we've gotten more and more new customers. It's now not unusual to have orders for 2 or 3 customers (new ones) per day, and this has been going on for a few weeks. This means they also have to increase their stock proportionately. This is why shelves are being put up in the cellar and stock there re-aligned so it will be able to hold more for the big lines. We also got in a small shipment of assorted merchandise from Lisa Monet. Some fill-ins were also received from the G. E. Madison Stores, here in Connecticut, and I learned that is the same firm as Dept. Sales Co., the outfit Moore does a lot of business with.

9/23/65 Although we didn't have many orders today, the bosses were anxious to get them done before Noon, and we did manage to get them completely filled and checked by that time.

After lunch, I was put to work at building shelves in the basement, with Aldo (from the O.T.C. Department) helping me. I know I did a good job on that and Mr. Moore himself said as much, again saying I worked faster than any carpenter they could hire. Mr. Moore seems to think highly of me. He also said he plans to have me build a lot more shelving because he will carry more lines and increase his stock of most companies he alreay stocks. A lot of Lilly merchandise came in today but I was downstairs when it was delivered, so I don't yet know where it was from.

9/24/65 I spent a good part of the day building shelves downstairs and, except for one section, have completed them. Mr. Moore said he'd like me to come in and finish them tomorrow, and I said I would. Rosow today brought in McNeil and Geigy merchandise. The McNeil consisted of 4 large repacks and covers the whole line, except

for Butisol Sodium and the other items that were on the first invoice I sent you. Of these original items, we still have a lot on hand, so they won't order any more of that unless they can get special prices on it. The Geigy that came in was again the full line and mostly the 1000's sizes of the different items. All told, there were 8 large repacks on that and I would estimate its worth as between $15,000 and $20,000.

We also got in 181 cases of Robins, delivered by the M.E.M. Trucking Company of Massachusetts (the City name wasn't too legible on the truck, but it may have been Leopoldville). This was addressed to H. L. Moore, but another label had been cut off before Moore's was applied. From the cut, the size of the label must have been 1½" x 2½". This definitely wasn't the Webster or Lisa Monet label, but it could have been Rosow on the small label. Last week, though, Sam told me he had ordered Robins from Minnesota, so I have no other data on today's delivery. We still haven't gotten any more Johnson & Johnson in but, when we do, it is all Robert Wood Johnson. We are still moving much more of the cosmetics and perfumes than we do on drugs. Cosmetics always come in 300 case or more lots, which are immediately taken into the Cosmetics Room, where the labels are cut off as quickly as possible.

Mr. Rosow himself (the older one) came in today, but I didn't see him. I was speaking with Jerry Rome when one of the boys came over and said Mr. Rosow was upstairs and wanted to see him. Jerry Rome, who usually acts as though he owns the place, dropped everything and went running up to see Mr. Rosow. We are still getting more and more new account orders, very few for

less than $2,000, and especially for Lilly, Smith Kline & French, Robins and Ciba. These orders are mostly coming from pharmacies in North and South Carolina, Tennessee, Alabama, etc. Sam Moore is still asking Jerry Rome how to do things. He is also the one who tells Rome when it is time to order more merchandise and Rome handles the placing of those orders himself, so it seems he's the one with the connections with Webster, Rosow, etc. Rome handles so much here that he makes Hy Moore seem only to be the "figure-head," as far as getting that kind of merchandise is concerned, as Rome is the one who decides when to buy, where from, and how much. Now, whenever Mr. Moore sees me move cases, he tells Sam to get one of the kids to do that, that I'm too valuable to use for that. Mr. Moore has also said he wants to move me "up" in the Company. The Wallace export merchandise we got in recently is being pushed out fast, in fact, when we have an order for the 1,000 size of one of those items, instead of taking a bottle of 1000's from other stock, we send out 10 bottles of 100's, from this export shipment.

9/27/65 This was a busy day here and especially so, due to the Holidays, because Mr. Moore, Sam, Jerry Rome, Mr. Goldfarb, Mr. Wolf and Mr. Burkowitz were off. M. & M. delivered, from Lisa Monet, Inc. a Lilly shipment. This consisted of $4,394 of Darvon Compound 65 in 500's, 16 X 5000 Tuinal 3 Gr., 6 X 5000 Seconal Sodium 1½ Gr., and 9 X 5000 Tuinal 1½ Gr. Adley Express Co. also delivered 95 cases of Cepacol, which I believe was sent direct to Merell Company. Rosow also brought in 230 cases and 6 repacks of Warner-Chilcott which represented their full line,

except for bulk goods. Besides the Rosow label we cut off that, another label had been cut off before the Rosow label was applied.

They also delivered, at the same time, 9 repacks of Geigy. We also got in 4 repacks of Roerig. On that, a label is enclosed, stating it was sent from the Chas. Pfizer & Co., 230 Brighton Road, Clifton, New Jersey, on Invoice No. 830849, UBA3, addressed to H. L. Moore Drug, here on Arch Street. We also got in Pitman-Moore and Poythress, but those came direct. Incidentally, H. L. Moore also sells, under its own label, such items as Phenobarbital, Meprobamate, and one called Tetramets (which is Tetracycline). I overslept last Saturday and didn't come to work, and today Moore said it was just as well that I didn't because they only worked until 10:30 A.M. and then closed and went home.

9/28/65 We only had a moderate amount of orders today and nothing much happened. The only drug shipment that came in today was from National Drug, and it came direct. When Sam and I discussed Wallace items today, he again said the last shipment was export and was delivered here during the middle of the night. Incidentally, some of the H. L. Moore merchandise, showing their name as distributor, is sold under the label "C.V.C." which I believe is Central Vitamin Corporation. This firm supposedly has branches in Long Island and New Jersey, but Lisa Monet has delivered that stuff to us in the past. Until now Moore was selling Tetracycline under that label. Now, though, they just came out with it under the name of Tetramets, under the C.V.C. label.

The other items under Moore's name, like Pred-

nisone, etc., are made by the Zenith Pharmaceutical Corporation in New Jersey, and their merchandise has also been sent to us by Lisa Monet. Moore is having a new catalog printed, to include many more Lilly and other items. Jerry Rome and Hy Moore have also told me that they will be getting more Lilly items soon (the full line) and that's one of the reasons they need the additional shelves in the basement. Jerry Rome and Hy Moore were in for only a few hours today, but none of the other Jewish personnel came in.

9/29/65 Today we again weren't too busy, so I finished making the shelves in the basement. While I was down there, some more Warner-Chilcott came down and Sam Moore immediately cut the labels off the cases. I found some portions of the cartons, on which some name and address had been marked-out in Black ink (eradicator indicates this name was McKesson & Robbins, Newfield Avenue, Hartford, Conn.). The number "118" had also been written on this. What we got in was about 40 cases, mostly prescription items. We also got in a shipment of Synthroid Tablets (made by Flint Labs.), but I didn't find any of those discarded labels. In that, there were 32 dozen Synthroid 0.2 Mg. 500's, 436 of the 0.1 Mg. 500's, and 50 0.1 Mg. 100's. Everything else was quiet here today.

9/30/65 Nothing of interest happened here today. In fact, it was such a slow day that we spent most of our time putting up stock. Sam, though, spent the day on the telephone, ordering and buying merchandise. We didn't receive even one drug delivery, and only a few cases of cosmetics, but I don't know where from.

10/1/65 This was also a very slow day for us.

We finished our orders and put up all the stock we had by 1 P.M. When I left the place at 1:45 P.M., 17 or 18 repacks of Smith Kline & French merchandise had just been brought in. I don't know who brought these in, but they were all stamped "H. L. Moore, 610 Arch Street, New Britain, Connecticut." These looked like S.K.F. repacks and looked almost as though they had come straight from S.K.F.

Earlier in the morning, Rosow brought in 70 cases of Lilly merchandise, 64 original cases and 6 repacks. Of that, about 35 consisted of Darvon Compound, 32 Mg. and Darvon Compound-65, in 500's sizes. The balance was a little each of the remaining Lilly items we carry, including 2 cases of each Insulin, packed 72 pieces to a case. I noticed that on the Wallace "export" shipment, there were dates and stamped numbers on the outside cases, but I couldn't get near enough to them to see what they were. Jerry Rome said that although we now carry some Polaroid items, he is trying to get in their full line, including many films, particularly color film.

10/4/65 Except for a short while this morning, we weren't too busy. Mr. Moore called me into his office and asked if I would be willing to build some more shelves, as they need more room for cosmetics and perfumes for the Christmas Season. I told him I'd be glad to make some more. Although I wasn't able to secure a copy of it yet, a special mailing went out today. Four of the specials were on McNeil merchandise, on the Butisol Sodium ¼ and ½ Grain in 1000's, the Syndrox 1000's, and Butibel 100's. These items are still some of the oldest shipment (possibly export) and were put on special because they ap-

parently are not moving out fast enough. Besides those, we also have about 6 Parke Davis items on the special.

10/5/65 Since we again weren't too busy, Mr. Moore had me start building shelves in the Cosmetics Room. He again explained that with Christmas coming, we would get in more cosmetics than we usually stock, and much more than we really have room for. We received a shipment of Bristol-Myers goods, 232 cases, from En-Bee Drug Co., which Mr. Moore told me was a special shipment. This consisted of Bufferin, Score, bath oil and other over-the-counter items. Lisa Monet also sent in a shipment of cosmetics, but this also included about 60 cases of Mead Johnson merchandise, mostly their Oracon, Colace and Peri-Colace. We also got in a Bristol Labs. shipment, from Sobel, totalling $7,184.00 on the invoice. Bristol had always come in in the original cases, which were stamped "H. L. Moore," so I assumed they were direct shipments, but this was definitely from Sobel, as I saw the invoice with his name on it. When I checked that special Wallace shipment today, I found bits of paper on it, with one line that had "O" as the second and fourth letters on the line. The other letters on that line, as well as those on the second line had been torn off, but the third line started with an "N," so it's possible this was the name of the supplier (possibly Rosow and Newington).

Enclosed is a copy of the new specials catalog. In addition to the McNeil and many other items, note that this also offers Wallace merchandise at special 15% discount, and these are the Wallace items we got in that special shipment. Today Mr. Moore again reminded me that he is getting in a

lot of cosmetics and perfumes and he said he is getting a lot of free goods with it. When I told him I would also be glad to help check that merchandise in, he said I could learn in time but to stay on drugs while we're busy there, since I don't yet know the perfume prices and would like more time to check them for the different small sizes, such as ¼, ½ ounce, etc. While we don't do much on Max Factor, Moore's biggest business is done on items from Dana, Faberge, Chanel, Lentheric (Colognes only), Tussy, Revlon (all items), and on certain Helena Rubinstein items, such as Skin Dew, etc.

10/6/65 Because of the Holiday, none of the bosses were around, so we had a quiet day. We received a Webster Drug shipment, from Webster Drug in Minneapolis, to Webster Drug at this address. In the shipment were 96 cases of Warner-Chilcott merchandise. The invoice price on that was $13,675.72. On the bottom of the invoice and packing slip, someone had written in "H. Boxer" in red pencil. In the same shipment, we also received 16 cases of Syntex merchandise, with an invoice price of $4,004.00. We also received 17 repack cases of Helena Rubenstein merchandise from Midtown Drug, 566 Farmington Avenue, Hartford, Connecticut. From Biddle Purchasing Co. we received 4 cases of Lilly merchandise. It looked like En-Cebrin or En-Cebrin-F, but I won't be sure of that until it is unpacked. I learned that we got in another National shipment yesterday, but that came direct, as all of their merchandise has since I've been here.

Enclosed is a label I found on a Merck Sharp & Dohme shipment. Label reads: "From: Merck Sharp & Dohme, 40 A Street, Needhom Heights,

Mass. 02194 — Parcel Post — to D. A. Rosow, Inc., 184 Fenn Road, Newington, Conn." The last Merck Sharp & Dohme shipment we got in two days ago also came from Rosow, but this is the first time I saw, and secured, one of his labels on it. I've noticed that Moore never places an order for any particular Merck Sharp & Dohme items, they just accept anything Rosow or anyone else can send them on it. A few days ago, I heard Mr. Wolf say he'd have to order more cosmetics and perfumes from some one named Howard (first name either Steve or Bob) and he said he would call him (this is possibly connected with the name "R. Howard" listed under the Lisa Monet, Inc. name at the 89 Tec Street, Hicksville Building).

Incidentally, on the Emko "export" shipment we got in a while ago, a day or two after it came in, we sent 30 to 40 cases of it to Dept. Sales Co. under the name "Medicine Drug Stores." I learned that Axelrod's Pharmacy which is at the same address as Dept. Sales Co. is supposedly owned by Mr. Axelrod who is a close friend of Hy Moore's. Hy Moore also told me he owned that store in the past. I also learned that when we get merchandise from Dept. Sales Co. (especially in large quantities on cosmetics, etc.) it comes in to us under that name. But, we also sell them merchandise from here (mostly Lilly Darvon Compound Seconal, etc. and Mead Johnson and Warner-Chilcott merchandise), which they buy about $1,000 at a time, but when we send them merchandise we sell it to them under the name "Medicine Drug Stores" or "G. E. Madison Drug Stores."

10/7/65 Today I was again building shelves in the Cosmetics Room, but no cosmetic ship-

ment came in today. Mr. Boxer today came in with 19 full cases and 1 repack of U.S. Vitamin merchandise. Although that merchandise was addressed directly to H. L. Moore, Boxer delivered it in his Cadillac. He also delivered 12 dozen Mead Johnson Oracon which was not in any way stamped or labeled. At the same time, he also delivered 2 cases of Moore private label merchandise. Boxer seems to be rather chummy with Burkowitz and call one another by their first names. Today they were talking about a bottle of something Boxer was supposed to bring him (I couldn't make out what this was, except that they kept referring to "a bottle," but I got the impression they didn't mean liquor). I've noticed that the Moores treat Burkowitz gently but, since he does handle all their shipping, he must also know about the deals they pull. They also placed a few orders with Boxer today, one of which I believe was for Smith Kline & French merchandise, but the goods involved won't come in here for another week or so.

Rosow today delivered a load of Wyeth S.M.A. Liquid, 50 or 60 cases of it. However, since all bulk loads are being delivered to Burkowitz in shipping, and he checks in all the bulk, I had no chance to examine any of these cases. Today I learned that Burkowitz has been checking in all the bulk shipments, including Johnson & Johnson's and Mead Johnson's. While down in the basement with Hy Moore today, I saw a lot of Micrin, so I remarked to him that I didn't remember seeing so much of it come in. He said that Burkowitz had checked it in and that all bulk goes to him, instead of to us up front, because to check all that in would take too much of our time.

On many of the Micrin cases I saw, the En-Bee Drug name was on them. Today we got from En-Bee Drug a shipment that was addressed to them and which had been sent to En-Bee from the Chas. Pfizer Co., Clifton, New Jersey. That consisted of 120 cases of Desitin 1 ounce (packed 2 dozen to a case), 8 cases of the 4 ounce size (packed 6 dozen to the case), one repack case, and 1 case of suppositories that possibly contained 4 dozen pieces. The En-Bee Drug, on the Pfizer label, showed the address as 31 Wilson Street, New Britain, Connecticut.

Today they hired a college fellow to work here part-time, after school. He will be working with Sam Moore because when Sam fills orders (in the S through Z Drug Aisles), he likes to read off the names of the items, while someone else actually picks them. He also likes to be the only one who works the sections he normally handles, so I haven't been able to get to pick in those areas yet. Last night we got in some Chilton Labs. Enerjets last night, but I don't yet know who shipped them in, but there were 25 to 50 vials of it involved. Moore still seems to get in new items as soon as manufacturers come out with them, and this includes the latest Bristol and Ciba items. Rosow is still making all his deliveries here in his unlettered panel truck, usually driven by a young, lanky, hill-billy-looking blond fellow, but the goods he delivers in it are usually plainly stamped with the Rosow name. We are still pushing out the Wallace export merchandise and continue to fill orders for their items by shipping 10 bottles of 100's, of this export merchandise, when some one asks for 1000. Today I noticed that we got an order from another new customer, Some

Pharmacy, a retailer, in Spartanburg, South Carolina. Hy Moore now evidently trusts me completely as he is now telling me how they will set up merchandise in the cellar. He also dropped a hint about giving me another raise.

10/8/65 Today we got many, many shipments in. As far as I was able to determine, the following lines came direct: 48 cases of Dorsey, 150 of Norwich Labs., Riker and Merrell. Although the Merrell shipment looked as though it came direct, it may not have been, because it was written-up on a plain piece of paper, such as Rosow, Webster, etc. use, and it was not on a Merrell invoice the way it normally is. We also got from M. Sobel, Inc., 507-509 East 165th Street, Bronx, New York: 170 cases of Roche (the full line) and another 100 cases or so containing the following: Merck Sharp & Dohme, Lederle, Lilly, Schering (the full line), and Roerig, which had the Pfizer label on it. Actually, I wouldn't have known all that was from Sobel, but Jerry Rome called out over the intercom that they needed help to unload about 300 cases which Sobel was delivering. Rosow also delivered 5 repacks of Geigy, containing only their Dulcolax Suppositories 4's, which we had been out of for some time.

Incidentally the Merrell merchandise I mentioned above was 92 cases of Kolantyl-Gel, which was delivered to Moore by Allied Shipping. From Goldberg's Department Store in New Britain we also got in about 20 repacks of Helena Rubinstein goods and about 30 repacks of Jade East Gift Sets, from which the labels had been cut off. Those shipments came in so fast that I wasn't able to get any more details on them. I saw that a lot of cosmetics were also brought up from the

basement today, all of which were marked "Dept. Sales Co.," but I don't know how long these were down there or what the cases actually contained in those lines. Today Hy Moore asked me if I'll be able to bring my parents into the Country soon. He said he hoped so, as he wanted me to remain happy here and not possibly return to California. He also said that if I was having trouble getting the visas to let him know, because he's very friendly with the Governor of Connecticut and also with a senator. I told him I'd be sure to let him know if I couldn't work it out myself.

10/11/65 This was another busy day for us, but everything went smoothly. We got in 2 repacks of Geigy, containing mostly Preludin in the 1000's size, and it came from Grismonde, 112 Country Road, Fairfield, Connecticut. Webster Drug delivered 34 cases of Ortho-Novum, 2 Mg., 20's, dial pack. The labels that were on those cases, prior to Webster's, had all been cut off. We also got in 30 cases of Robins Quinidex Tablets 30's and 7 cases of Dorsey Triaminicin 12's. The only thing I know about the last two is that they were delivered on a truck bearing New York license plates. I believe I've seen that truck here before and possibly it was Mid-Atlantic's. Rosow delivered the full Ayerst line, consisting of 6 large repacks, and 72 of the 100's of Geigy's Preludin Endurets and 4 of their Sterazolidin 1000's.

We also got in the largest Bristol Labs. shipment I've seen here so far, 27 large repack cases measuring about 2 cubic feet each, which came from Maddy Drug & Sundries, 315 North Jefferson, Syracuse, New York. We also got in 50 cases of Borden Pharmaceutical's Mull-Soy Liquid, but that was bulk goods and went to Burkowitz,

so I don't know where it's from. Today I spoke to Mr. Goldfarb from the Tab. Room. He asked me how Brunswig in California ran their operations and kept their records. I told him everything was done on computer machines and with I.B.M. Systems, which he said they couldn't do here. I said I was fascinated with what he was doing in the Remington Rand Office, so he said if I wanted, I could come in during lunch or when I have extra time and he will teach me their system. Hy Moore heard that and said he also thinks it would be a good idea to teach me how they work that end of the operation.

10/12/65 Today we filled 87 orders, each of which averaged about $1,000 and Mr. Goldfarb said this was the most they had ever done on a Tuesday in the history of Moore Company. The only thing we got in today, Columbus Day, was one shipment from En-Bee Drug, consisting of Helene Curtis goods — 8 cases of the large size Tender Touch, and 7 cases of their Suave Hair Dressing. Everything else was quiet.

10/13/65 Today Hy Moore promoted me to the job Sam was holding down, namely that of being in charge of the entire Rx Filing Department. Sam is now only supposed to do desk work, like ordering and figuring out what has to be ordered. This job won't give me as much time to check-in merchandise, but I will continue to check some and, of course, will have the time to seek-out some information on that end. I will also continue to check some out-going orders, and will have a good opportunity to check the merchandise coming into the sections. Sam Moore is now unhappy because he isn't supposed to leave the desk, whereas he likes to get involved in every-

thing so he'll know what is going on. Hy Moore is now spending most of the day on the telephone, as is Jerry Rome who apparently is still handling all their "under the table" transactions. I will now pick from the last aisle and will also check what all the other pickers filled, but I will myself fill orders on: Smith Kline & French, Sherman, Squibb, Strasenburgh, Stuart, Syntex, Walker, U.S. Vitamins, Wampole, Warner-Chilcott, Wallace, White, Searle, Wyeth, and Winthrop, and also Warren-Teed.

I've noticed that when Sam Moore orders by telephone, he never mentions the names of the people he's speaking to. Even though Rosow brought in an Ayerst shipment on Monday, today we also got in a full Ayerst shipment, of the full line, from Alton Products Company, 159 Norfolk Street, Dorchester, Massachusetts, consisting of 15 or 16 cases. This is the first time I've seen anything with the Alton name on it, and we are now over-loaded with Ayerst Products. Biddle Purchasing Company today sent us fill-in shipments on: Searle (960S refills of Enovid-E #98 and #98 240's refills), 2 cases of Merck Sharp & Dohme, Pitman-Moore (possibly Neo-Polycin Ointments), and some of Parke Davis. Rosow delivered Lilly's Seconal Sodium, 1½ Gr. 5000. Rosow also brought in Geigy merchandise: 12 x 100 Hygroton, 25 x 1000 Torfranil, 25 Mg., and a few more single pieces of assorted items.

We also got in Burroughs Wellcome merchandise from Standard Drug in Detroit, Michigan. All labels had been removed from the cases, but I found the original packing slip and it is enclosed. Packing slip indicates this $2,700.00 Burroughs Wellcome shipment was sold to Standard Drug

Co. (no street address shown) in Detroit, by Frank W. Kerr Co., 1734 W. Lafayette, Detroit 16, Michigan, and totalled 1216 pieces. We also received 8 repacks of Countess Maritza Cosmetics. These repacks were very large and since they had a New York address on them, I believe they came direct. Biddle today also sent us 2 cases of Lentheric Colognes. Tonight Sam Moore made a local call, and while I couldn't make out what number he dialed, I believe it was Rosow, to order fill-ins on Stuart, Lilly, U.S. Vitamin, and possibly one other line.

The only time I've heard Sam Moore ever mention a name during a phone conversation was when he calls one particular point (which he does) every few days and then he calls the other party "Frank." Many times I have also heard Hy, Jerry and Sam say to call "Frank" to discuss things with him on the phone, but I've never been able to get close enough to hear what they tell him. I checked our Emko stock and didn't find any of the 129Gm. in stock, though it could have gone out the day after we got it in, in the shipment that went to G.E. Madison Stores. Lisa Monet today brought in some Mead Johnson merchandise, 2 cases of 15 cc. Tri-Vi-Sol (6 dozen to a case) and 4 cases of Tri-Vi-Sol 100's (4 dozen to a case). Sam told me that wasn't our regular Mead Johnson shipment, only a fill-in. We often have salesmen come in here, but so far I haven't been able to identify them. One, though, always seems to discuss only Mead Johnson merchandise, and another I believe is a Rosow salesman.

We are expecting a lot of bulk merchandise to come in this week sometime on Smith Kline & French, Mead Johnson, and possibly some oth-

ers. I think Moore is having trouble getting McNeil merchandise now. Today they were also discussing the possibility of taking in another special Wallace shipment, one they are considering purchasing. When I asked Jerry Rome what he meant by "special," he said the items they keep in the other room, "the export goods." They said that if we can make room for it, they will probably make the deal for it. The other day they also said they might get in a special on Lederle, but only on a few items, and that will also be put into a special place. The Wallace "export" merchandise is also still kept separately.

10/14/65 This morning Sam tried to get back to his old job of filling orders, but Hy Moore promptly got after him and told him to remain at the desk. Although it isn't so, Sam keeps saying the orders are moving much slower since he left picking. They have been going through a little slower, but only because we had so many more orders than usual this week. On Monday, we filled about 70, 87 on Tuesday, 76 on Wednesday, and close to 80 again today, mainly because of the great many new customers ordering this week. Rosow today delivered a mixed shipment, the goods Sam ordered last night, consisting of Lilly Insulin, McNeil Butisol Sodium Elixir, Mead Johnson Vasodilan in 1000's, Smith Kline & French's Stelazine 2 Mg. 500's – 1 dozen, 2 dozen Combid 50's and 2 bottles of Stuart's Dialose-Plus 500's, 2 cases of Winthrop Neo-Synephrine ½ a/c, ½ ounce, Nasal Spray, and 12 Searle Enovid-E Compact Refills #98, 240's. Those figures may not be exact, but they are as close as I could possibly make out.

Spector Mid-States today delivered to Webster

Drug Co., at Moore's, a shipment of 96 repack cases of Lilly merchandise, our regular shipment, which I believe came from Minneapolis. That consisted of a lot of the Darvon Compound-65, #369, in the 500's size. I couldn't see what else was included, but it was our regular Lilly shipment, and Sam said it was invoiced at $30,000. I saw that the Ayerst shipment we got in from Alton yesterday had an invoice price of $997.00. Today R.E.A. Express delivered to us 10 large repacks of Geigy (each repack holding about 10 dozen), from R. McGlone, 25 Lois Street, Manchester, New Hampshire, of which one label is enclosed, and this was addressed to H. L. Moore Drug Co. This represented the full Geigy Line, mainly 100's and 1000's, on Sterazoldin, Hygroton, Tandearil, etc. I only glanced at that invoice but was sure I saw twenty-two thousand and some odd dollars on it. We got in 98 cases of Glenbrook Labs. merchandise, from En-Bee Drug Co., assorted items, including Bayer Aspirin.

Incidentally, most of Moore's O.T.C. items are still stamped with the name of "En-Bee Drug Co.," so it seems they don't even bother cutting them off the over-the-counter merchandise any more. Warner-Chilcott merchandise also came in, from Lisa Monet, Inc., $2,200 worth, consisting mainly of bulk and fill-ins, such as: Agoral, Sinutabs, and some Peritratres. With that, Lisa Monet also sent in $2,500 worth of Young's Rubber Products. From G. E. Madison, we got in two or three dollars less than $10,000 of Dana Products, consisting of about 30 repacks of Dana's Ambush, Tabu, 20 Carats, etc., the full line we carry on them. Most of it, though, was sets for Christmas selling. These repacks measured about a yard

square, each, and had no markings of Dana's on them. However, the invoice had the Dana name at the top of it, and was made out to G. E. Madison Stores.

Hy Moore himself checked-in that shipment, and the labels were being cut off the cases. The picking in my section went well today. They hired two more college boys to work here every day after school and I am instructing them on how to re-arrange stock in the basement. Sam again complained to me today that he wants to pick and said his brother Hy is crazy, that even though Hy is always wrong, he has to be right, as he is the boss. Jerry Rome is still very friendly towards me, although he and Hy Moore don't discuss all phases of the business with the help, as Sam does. However, when I ask Jerry something, he answers me without any hesitation. Today, for instance, I asked him if any Lilly Multi-Cabrin came in. He said no, that's in "a special shipment," not in the regular shipment that comes from Webster (such as we just received).

Although only the Webster label was on this latest Lilly shipment, a large label, about 3″ long, had been cut off earlier. When I asked Rome what he meant by "special shipment," he said one like they got from Commons Bros. in the past. Jerry Rome still sits in his glassed-in office in the warehouse, directly across from me, and while I can sometimes hear his voice while he's on the phone, I haven't been able to make out anything he said. I have noticed that when he wants to discuss something very private, he goes into Hy Moore's office. Hy Moore's office seems old but I can't overhear anything said in there, so it's possible it's sound-proofed. Sam told me he is spending

$1,100 to rebuild his garage and asked if I would help him build some shelves in it when it's done. I told him I'd be glad to come to his house and help. Since Hy, Rome, Goldfarb, and even Wolf, seem to have more to say here than Sam, and they all use him as a scapegoat, maybe he'll open up and tell me something when I go to his home. They have a burglar alarm system here but each night, when the protection company's guard would try the door, the alarm would go off. The front door was so warped that when he touched it, it would set off the alarm, so I spent some time this morning putting a new bolt on the door to try to secure it.

A few remarks are appropriate here. In business, an employee's loyalty as well as his economic self-interest will help maintain security. The disgruntled employee, on the other hand, can do irreparable damage to the company he believes has cast him aside for one reason or another. Length of service is not equivalent to loyalty. It took a Seattle firm many months to discover that sporadic incidents of sabotage were the work of a long-time employee bitter over the death of a fellow worker in an industrial accident.

Talk, being cheap, is freely dispensed all too often. If it is too freely dispensed it may become trade gossip, an item in the trade press, or a cocktail party conversation piece. Two or three such items, if put together, may allow the competitor to pierce the secrecy.

Education is one effective countermeasure. Appropriate personnel should be given basic lectures by security personnel, by a law enforcement officer, and/or electronics specialist. They should

be made aware of the small size of equipment and the variety of potential hiding places for transmitters, and they should be impressed upon to check the credentials of repairmen and telco men. They should be trained to report the presence of suspicious or unauthorized people in highly secure areas, or even loitering about such areas. Unfamiliar people should be deemed intruders unless accompanied by an officer or manager.

In 1965 a self-avowed industrial spy divulged to *Business Management* magazine some of his techniques. Here is what he listed in the order of their simplicity:

(1) The use of what espionage experts call "resources in place," trusted employees already inside a sensitive area. The spy preferred bribing them, but he also might play upon their need for vengeance.

(2) Employing call girls to trick information out of someone who has it.

(3) Attaching eavesdropping devices to telephones or rooms.

(4) Impersonating factory workers, electricians, policemen, etc.

(5) Bribing someone to let him wander after hours through office or plant.

(6) Secretly entering a restricted area and photographing or inspecting the desired documents.

Note that this IE agent ranks electronic eavesdropping as his third easiest technique.

All personnel should be cautioned about discussing sensitive matters of any kind over the telephone or in public. Casual conversation over drinks can reveal trade secrets, unpatented innovations, designs and marketing information,

and future plans. Shop talk should be confined to the shop. During World War II the government posted signs with the warning, "Loose lips sink ships." It was a deadly metaphor.

In addition to electronic devices, careless employees and two-faced personnel, a major threat to the security of information is the common wastebasket. Take this example as cited in *Machine Design:*

> A company became suspicious of a competitor who suddenly began selling similar products at a lower price, and also was attempting to lure away salesmen. They were pretty sure that some of their engineering secrets were being stolen and began checking out their own personnel. Through financial profiles of employees, they found one man who appeared to be a likely suspect. The puzzle was that this man had access only to a portion of the secrets involved.
>
> They decided to put the man under surveillance anyhow, and soon had enough evidence to get a confession, which cleared up the mystery. The man was passing information to the competitor through an undercover agent who was also "buying wastebaskets" from the engineering department. The wastepaper was being supplied in coded bags to the agent. Surveillance of the janitor produced the evidence indicated by the confession, and broke up the spying operation.

The lesson here is obvious, to which it should be added that many firms are careless enough to leave discarded material collected from its

offices in outside containers awaiting pickup. Here it is readily available to any outsider utilizing what the FBI calls a "trash cover," which is no more than a close inspection of discarded material. One way to overcome this vulnerability is to burn all documentary trash. Another is to use paper disposers. One source markets a desk-size shredder. Another has a maximum-security shredder that cuts paper into 1/32 inch strips at a rate of up to 150 pounds per hour, and a casters-mounted shredder that will destroy up to 550 pounds per hour. There is also a breed of disintegrators that use water and chemicals or a hammer-mill process to reduce paper to pulp form.

Physical plant protection should be utilized. Barriers can prevent intrusion — gates, fences, guard shacks, etc. Inside the building, some areas should be declared off limits. Doors, files, and desks in sensitive areas should be locked and keys given out with discretion.

Since industrial espionage has been estimated as costing the business community billions of dollars a year, it follows that even a small businessman should be aware of the dangers and be prepared to prevent any leaks in his organization that might benefit his competitors, or even bankrupt his own company.

PART III

THE LAW

If you discover you've been victimized by electronic snooping – and have evidence to prove it – you may have legal recourse. The Omnibus Crime Control and Safe Streets Act of 1968 not only provides criminal penalties for nonlaw enforcement tapping and bugging but authorizes the recovery of civil damages. Moreover, there is the possibility of an invasion of privacy suit and, if the telco is involved, a breach of contract action.

The authors of the act take note of the pervasiveness of electronic surveillance: "There has been extensive wiretapping carried on without legal sanctions, and without the consent of any of the parties to the conversation." The same with bugging. "The contents of these communications and evidence derived there from are being sued by public and private parties as evidence in court and administrative proceedings . . ."

The solution to the problem, as envisioned by Congress, was to prohibit not only the interception and disclosure of wire or oral communications, which was accomplished by updating Sec-

tion 605 of the Communications Act, but to forbid the manufacture, distribution, possession, and advertising of devices for the interception of communications.

But at the same time Congress negated much of the effect by authorizing under the act wiretapping and bugging on the part of federal, state, and local law enforcement under court supervision in specified types of cases. These chiefly concerned "national security," an amorphous term unilaterally described by the government bureaucracy, and organized crime related investigations.

The electronic surveillance provisions of the act, which constitute Title III of Public Law 90-351, are published as Appendix A. Suffice it here to make a few observations.

It does not seem that the act will drastically alter the pattern of electronic espionage in the United States. To be sure, the more blatant advertising has been intimidated out of print. But the law has a large loophole as far as manufacture, distribution, and possession is concerned. It declares that the culprit must have reason to know that the device is designed so as to be "primarily useful for the purpose of the surreptitious interception of wire or oral communications." Since wireless mikes have long been promoted for such euphemistic purposes as baby-sitting, party fun, and intrusion prevention, and are legitimately used in the electronic media and at public meetings, the difficulty of proving a person's primary intent is readily apparent. The situation is similar also to the gun control provisions. There are so many electronic devices at large in this country, as there are guns, that the immediate cessation

of manufacture would hardly put a dent in the problem.

Some commentary is appropriate. First of all, the term interception is interpreted to mean, according to the law's legislative history,* an "aural acquisition of the contents" of a communication. This means that the pen register, or dial pulse register, is specifically excluded from the law. The authors of the law say they intended to protect the privacy of the communication itself, not the means of communication.

Secondly, the law is not intended to override state laws prohibiting interception. What this means is that in those jurisdictions where tapping and bugging is outlawed even for law officers, it will still be outlawed. However, it will not be illegal for officers to be in the possession of eavesdropping equipment, the reason being that they may legally eavesdrop with the permission of one of the parties. This happens quite often in obscene phone call cases, where it is desired to apprehend the culprit while he is making the call.

---

* *The full interpretations will be found in U.S. Code, Congressional and Administrative News, 90th Congress, Second Sessioin, 1968, Legislative History, pp. 2153-2163 and 2177-2197.*

At this early stage there have been a few prosecutions. One worth looking at took place in a Reno, Nevada, federal court and resulted in the conviction in November, 1970, of one Gordon Novel. Novel was working on behalf of a land developer trying to purchase land from Indians. Having learned of a meeting of Indian leaders,

he planted an attaché case mike-recorder under the building where it was to take place. It was found. It may be indicative of the government's tentative approach to prosecution that Novel was not charged with interception but with interstate transportation — the set was manufactured in Ohio — and possession.

The legislative history also reveals that the law is intended to be a model for state legislatures. Thus we may see a trend toward legalization of electronic eavesdropping for law enforcement and outlawing it for anyone else. The American Bar Association has formed a Special Committee on Standards Relating to Electronic Surveillance to help bring about that end. When its report was issued, only one member dissented. Declared Arthur J. Freund of St. Louis: "Wiretapping is one of the hallmarks of a police state."

The legislative history contains a passage betraying the difficulty of enumerating what devices are and what aren't primarily useful for interception:

> The prohibition thus will be applicable to, among others, such objectionable devices as the martini olive transmitter, the spike mike, the infinity transmitter, and the microphone disguised as a wristwatch, picture frame, cuff link, tie clip, fountain pen, stapler or cigarette pack. Such devices are widely advertised and distributed at the present time and are readily available on the market. By banning these devices, a significant source of equipment highly useful for illegal electronic surveillance will be eliminated.
>
> At the same time, the prohibitions of sec-

> tion 2512 will cause no substantial interference with the production, distribution, or use of legitimate electronics equipment, whether by the electronics industry or others. Size alone is not the criterion under the section. A device does not fall under the prohibitions merely because it is small, or because it may be adapted to wiretapping or eavesdropping. Nor will the prohibition be applicable, for example, to devices such as the parabolic microphone and other directional microphones ordinarily used by broadcasters at sports events. Such devices cannot be said to be primarily useful for surreptitious listening. To be prohibited, the device would also have to possess attributes that give predominance to the surreptitious character of its use, such as the spike in the case of the spike mike or the disguised shape in the case of the martini olive transmitter and the other devices mentioned in the previous paragraph.

What this seems to say is that the device has to be pretty blatant to be illegal.

Perhaps the most forboding aspect of the act is the legalization of electronic intrusion by law enforcement. All along, of course, agencies have done so on their own authority with their own rationalizations as to the public good to be served. The act seems destined to expand this activity. It can be expected that were court authority not forthcoming, some agencies would proceed without it. This if they even bother to seek court approval to begin with. Attorney General John N. Mitchell announced not long after the act went into effect that the Department of Justice

would snoop on its own authority in cases deemed to be "national security," thus undermining the cut of the act. And enforcement promises to be perfunctory. It is in the hands of the FBI, which was never very zealous in enforcing the Communications Act.

A bright spot for the citizen is the section authorizing recovery of civil damages. Section 2520 states in part: "Any person whose wire or oral communication is intercepted, disclosed, or used in violation of this chapter shall (1) have a civil cause of action against any person who intercepts, discloses, or uses, or procures any other person to intercept, disclose, or use such communications, and (2) be entitled to recover from any such person actual damages in a minimum amount, punitive damages and attorneys' fees and costs.

Civil recovery has been available all along in most courts, and the new law permits filing in federal court. An example of a state court civil suit comes in the IE case recounted earlier involving the planting of a microphone in the Redwood City, California, plant of Botts Line Co. After the M. C. Corporation president and his foreman who secreted the bug were convicted of conspiracy to overhear a private conversation and sentenced to four months in jail, Botts Line sued M. C. Corporation for $200,000.

Another basis for suit is invasion of privacy. This was one of the grounds of the Las Vegas casino owners' action against the Central Telephone Co. of Nevada after it leased lines to the FBI that were used to transmit bugged conversations. The suit was eventually settled out of court.

Pressing of criminal prosecution is yet another alternative, and it is sometimes an advantageous prelude to civil suit. As it stands now, anyone, including law enforcement officers, who intercepts without a court authorization, stands in violation of the act. Moreover, certain high-powered bug transmission may violate regulations of the Federal Communications Commission. It would be the unusual case that was not prosecutable under some statute.

The crimes that can be committed by an eavesdropper, depending on local laws, can be summarized:

(1) Electronic eavesdropping
(2) Possession of burglary tools
(3) Break and enter
(4) Trespassing
(5) Possession of eavesdropping devices
(6) Bribery
(7) Furnishing false identification; impersonating a police or federal agent.
(8) Attachment of foreign devices to telephone and power lines, tampering with utility lines.
(9) Conspiracy with client to commit any of above.

A final note should be added, one on the same chord that opened this book. The hearings of the Senate Subcommittee on Constitutional Rights, chaired by Sam Irvin, verified in graphic detail the pervasiveness of audio-visual surveillance in this nation. Members of Congress, among them Senators George McGovern and Birch Bayh, expressed the fear that their offices were

electronically monitored, and told how they operated on the assumption their phones were tapped. The state of the eavesdropping technology advances stride by stride with the advance of electronics. Now we have integrated circuits no bigger than the period at the end of this sentence. Laser technology has moved ahead to the point where government "spook" agencies already have used laser beams to induce vibrations and pick up sounds from rooms with drawn curtains. The Soviets hid a transponder device in the Great Seal of the U.S. in the American Embassy in Moscow, energizing it remotely.

These developments are ominous. As George Orwell wrote in *1984* in an all-too-prescient projection of future life in the spy state: "There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork . . . You had to live – did live, from habit that became instinct – in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized."

REPRINT OF TITLE III: *The Law Covering Wiretapping and Electronic Surveillance.*

Findings

Sec. 801: On the basis of its own investigations and of published studies, the Congress makes the following findings:

(a) Wire communications are normally conducted through the use of facilities which form

part of an interstate network. The same facilities are used for interstate and intrastate communications. There has been extensive wiretapping carried on without legal sanctions, and without the consent of any of the parties to the conversation. Electronic, mechanical, and other intercepting devices are being used to overhear oral conversations made in private, without the consent of any of the parties to such communications. The contents of these communications and evidence derived therefrom are being used by public and private parties as evidence in court and administrative proceedings, and by persons whose activities affect interstate commerce. The possession, manufacture, distribution, advertising, and use of these devices are facilitated by interstate commerce.

(b) In order to protect effectively the privacy of wire and oral communications, to protect the integrity of court and administrative proceeding, and to prevent the obstruction of interstate commerce, it is necessary for Congress to define on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized, to prohibit any unauthorized interception of such communications, and the use of the contents thereof in evidence in courts and administrative proceedings.

(c) Organized criminals make extensive use of wire and oral communications in their criminal activities. The interception of such communications to obtain evidence of the commission of crimes or to prevent their commission is an indispensable aid to law enforcement and the administration of justice.

(d) To safeguard the privacy of innocent persons, the interception of wire or oral communications where none of the parties to the communication has consented to the interception should be allowed only when authorized by a court of competent jurisdiction and should remain under the control and supervision of the authorizing court. Interception of wire and oral communications should further be limited to certain major types of offenses and specific categories of crime with assurance that the interception is justified and that the information obtained thereby will not be misused.

Sec. 802. Part 1 of title 18, United States Code, is amended by adding at the end the following new chapter:

Definitions

"As used in this chapter—

"(1) 'wire communication' means any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications;

"(2) 'oral communication' means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectations;

"(3) 'State' means any State of the United States, the District of Columbia, the Common-

wealth of Puerto Rico, and any territory or possession of the United States;

"(4) 'intercept' means the aural acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical or other device.

"(5) 'electronic, mechanical, or other device' means any device or apparatus which can be used to intercept a wire or oral communication other than—

"(a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a communications common carrier in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business; or (ii) being used by a communications common carrier in the ordinary course of its business, or by an investigative or law enforcment officer in the ordinary course of his duties;

"(b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal;

"(6) 'person' means any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation;

"(7) 'Investigative or law enforcement officer' means any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter, and any attorney authorized by law

to prosecute or participate in the prosecution of such offenses;

"(8) 'contents', when used with respect to any wire or oral communication includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication.

"(9) 'Judge of competent jurisdiction' means—

"(a) a judge of a United States district court or a United States court of appeals; and

"(b) a judge of any court of general criminal jurisdiction of a State who is authorizing interceptions of wire or oral communications;

"(10) 'communication common carrier' shall have the same meaning which is given the term 'common carrier' by section 153(h) of title 47 of the United States Code; and

"(11) 'aggrieved person' means a person who was a party to any intercepted wire or oral communication or a person against whom the interception was directed.

Interception and disclosure of wire or oral communications prohibited

"(1) Except as otherwise specifically provided in this chapter any person who—

"(a) willfully intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire or oral communication;

"(b) willfully uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when—

"(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

"(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

"(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

"(iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

"(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States:"

"(c) willfully discloses, or endeavors to disclose, to any other person the contents of any wire or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire or oral communication in violation of this subsection; or

"(d) willfully uses, or endeavors to use, the contents of any wire or oral communication, knowing or having reason to know that

the information was obtained through the interception of a wire or oral communication in violation of this subsection:

shall be fined not more than $10,000 or imprisoned not more than five years, or both.

"(2) (a) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of any communication common carrier, whose facilities, are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the carrier of such communication: *Provided*, That said communication common carriers shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

"(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

"(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire or oral communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

"(d) It shall not be unlawful under this chap-

ter for a person not acting under color of law to intercept a wire or oral communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution of the United States or of any State or for the purpose of committing any other injurious act.

"(3) Nothing contained in this chapter or in section 605 of the Communications Act of 1934 (48 Stat. 1143; 47 U.S.C. 605) shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government. The contents of any wire or oral communication intercepted by authority of the President in the exercise of the foregoing powers may be received in evidence in any trial hearing, or other proceeding only where such interception was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power.

Manufacture, distribution, and advertising of wire or oral communication intercepting devices prohibited

"(1) Except as otherwise specifically provided in this chapter, any person who willfully—

"(a) sends through the mail, or sends or carries in interstate or foreign commerce, any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire or oral communications;

"(b) manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire or oral communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce; or

"(c) places in any newspaper, magazine, handbill, or other publication any advertisement of—

"(i) any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire or oral communications; or

"(ii) any other electronic, mechanical, or other device for the purpose of the surreptitious interception of wire or oral communications,

knowing or having reason to know that such advertisement will be sent through the mail or transported in interstate or foreign commerce,

shall be fined not more than $10,000 or imprisoned not more than five years, or both.

"(2) It shall not be unlawful under this section for—

"(a) a communications common carrier or an officer, agent, or employee of, or a person under contract with, a communications common carrier, in the normal course of the communications common carrier's business, or

"(b) an officer, agent or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof, to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire or oral communications.

Confiscation of wire or oral communication intercepting devices

"Any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in violation of section 2511 or section 2512 of this chapter may be

seized and forfeited to the United States. All provisions of law relating to (1) the seizure, summary and judicial forfeiture, and condemnation of vessels, vehicles, merchandise, and baggage for violations of the customs laws contained in title 19 of the United States Code, (2) the disposition of such vessels, vehicles, merchandise, and baggage or the proceeds from the sale thereof, (3) the remission or mitigation of such forfeiture, (4) the compromise of claims, and (5) the award of compensation to informers in respect of such forfeitures, shall apply to seizures and forfeitures incurred, or alleged to have been incurred, under the provisions of this section, insofar as applicable and not inconsistent with the provisions of this section; except that such duties as are imposed upon the collector of customs or any other person with respect to the seizure and forfeiture of vessels, vehicles, merchandise, and baggage under the provisions of the customs laws contained in title 19 of the United States Code shall be performed with respect to seizure and forfeiture of electronic, mechanical, or other intercepting devices under this section by such officers, agents, or other persons as may be authorized or designated for that purpose by the Attorney General.

Immunity of witnesses

"Whenever in the judgment of a United States attorney the testimony of any witness, or the production of books, papers, or other evidence by any witness, in any case or proceeding before any grand jury or court of the United States involving any violation of this chapter or any of the offenses

enumerated in section 2516, or any conspiracy to violate this chapter or any of the offenses enumerated in section 2516 is necessary to the public interest, such United States attorney, upon the approval of the Attorney General, shall make application to the court that the witness shall be instructed to testify or produce evidence subject to the provisions of this section, and upon order of the court such witness shall not be excused from testifying or from producing books, papers, or other evidence on the ground that the testimony or evidence required of him tend to incriminate him or subject him to a penalty or forfeiture. No such witness shall be prosecuted or subjected to any penalty or forfeiture for or on account of any transaction, matter or thing concerning which he is compelled, after having claimed his privilege against self-incrimination, to testify or produce evidence, nor shall testimony so compelled be used as evidence in any criminal proceeding (except in a proceeding described in the next sentence) against him in any court. No witness shall be exempt under this section from prosecution for perjury or contempt committed while giving testimony or producing evidence under compulsion as provided in this section.

Prohibition of use as evidence of intercepted wire or oral communications

"Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency,

regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

Authorization for interception of wire or oral communications

"(1) The Attorney General, or any Assistant Attorney General specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of—

'(a) any offense punishable by death or by imprisonment for more than one year under sections 2274 through 2277 of title 42 of the United States Code (relating to the enforcement of the Atomic Energy Act of 1954), or under the following chapters of this title: chapter 37 (relating to espionage), chapter 105 (relating to sabotage), chapter 115 (relating to treason), or chapter 102 (relating to riots);

"(b) a violation of section 186 or section 501 (c) of title 29, United States Code (dealing with restriction on payments and loans

to labor organizations), or any offense which involves murder, kidnapping, robbery, or extortion, and which is punishable under this title;

"(c) any offense which is punishable under the following sections of this title: section 201 (bribery of public officials and witnesses), section 224 (bribery in sporting contests), section 1084 (transmission of wagering information), section 1503 (influencing or injuring an officer, juror, or witness generally), section 1510 (obstruction of criminal investigations), section 1751 (Presidential assassinations, kidnapping, and assault), section 1951 (interference with commerce by threats or violence), section 1952 (interstate and foreign travel or transportation in aid of racketeering enterprises), section 1954 (offer, acceptance, or solicitation to influence operations of employee benefit plan), section 659 (theft from interstate shipment), section 664 (embezzlement from pension and welfare funds), or sections 2314 and 2315 (interstate transportation of stolen property);

"(d) any offense involving counterfeiting punishable under section 471, 472, or 473 of this title;

"(e) any offense involving bankruptcy fraud or the manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotic drugs, marihuana, or other dangerous drugs, punishable under any law of the United States;

"(f) any offense including extortionate credit transactions under sections 892, 893, or 894 of this title; or

"(g) any conspiracy to commit any of the foregoing offenses.

"(2) The principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision thereof, if such attorney is authorized by a statute of that State to make application to a State court judge of competent jurisdiction for an order authorizing or approving the interception of wire or oral communications, may apply to such judge for, and such judge may grant in conformity with section 2518 of this chapter and with the applicable State statute an order authorizing, or approving the interception of wire or oral communications by investigative or law enforcement officers having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of the commission of the offense of murder, kidnapping, gambling, robbery, bribary, extortion, or dealing in narcotic drugs, marihuana or other dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year, designated in any applicable State statute authorizing such interception, or any conspiracy to commit any of the forgoing offenses.

Authorization for disclosure and use of intercepted wire or oral communications

"(1) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire or oral communication, or evidence derived therefrom, may disclose such contents to

another investigative or law enforcement officer to the proper performance of the official duties of the officer making or receiving the disclosure.

"(2) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire or oral communication or evidence derived therefrom may use such contents to the extent such use is appropriate to the proper performance of his official duties.

"(3) Any person who has received, by any means authorized by this chapter, any information concerning a wire or oral communication, or evidence derived therefrom intercepted in accordance with the provisions of this chapter may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any criminal proceeding in any court of the United States or of any State or in any Federal or State grand jury proceeding.

"(4) No otherwise privileged wire or oral communication interception in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.

"(5) When an investigative or law enforcement officer, while engaged in intercepting wire or oral communications in the manner authorized herein, intercepts wire or oral communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in subsections (1) and (2) of this section. Such contents and any evidence derived therefrom may be used under section (3) of this section when authorized or approved by a judge of competent jurisdiction

where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter. Such application shall be made as soon as practicable.

Procedure for interception of wire or oral communications

"(1) Each application for an order authorizing or approving the interception of a wire of oral communication shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:

"(a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

"(b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular discription of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;

"(c) a full and complete statement as to whether or not other investigative proce-

dures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;

"(d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

"(e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire or oral communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and

"(f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

"(2) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application.

"(3) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire or oral communications within the territorial jurisdiction of the court in which the judge is sit-

ting, if the judge determines on the basis of the facts submitted by the applicant that—

"(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter;

"(b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;

"(c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;

"(d) there is probable cause for the belief that the facility from which, or the place where, the wire or oral communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

"(4) Each order authorizing or approving the interception of any wire or oral communication shall specify—

"(a) the identity of the person, if known, whose communications are to be intercepted;

"(b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;

"(c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;

"(d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and

"(e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

"5) No order entered under this section may authorize or approve the interception of any wire or oral communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purpose for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days.

"(6) Whenever an order authorizing interception is entered pursuant to this chapter, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the auth-

orized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require.

"(7) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that—

"(a) an emergency situation exists with respect to conspiratorial activities threatening the national security interest or to conspiratorial activities characteristic of organized crime that requires a wire or oral communication to be intercepted before an order authorizing such interception can with due diligence be obtained, and

"(b) there are grounds upon which an order could be entered under this chapter to authorize such interception,

may intercept such wire or oral communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire or oral communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as pro-

vided for in subsection (d) of this section on the person named in the application.

"(8) (a) The contents of any wire or oral communication intercepted by means authorized by this chapter shall, if possible, be recorded on tape or wire or other comparable devices. The recording of the contents of any wire or oral communication under this subsection shall be done in such way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under his directions. Custody of the recordings shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing or denying judge and in any event shall be kept for ten years. Duplicate recordings may be made for use or disclosure pursuant to the provisions of subsections (1) and (2) of section 2517 of this chapter for investigations. The presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire or oral communication or evidence derived therefrom under subsection (3) of section 2517.

"(b) Applications made and orders granted under this chapter shall be sealed by the judge. Custody of the applications and orders shall be wherever the judge directs. Such applications and orders shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction and shall not be destroyed except on order of the issuing or denying judge, and in any event shall be kept for ten years.

"(c) Any violation of the provisions of this subsection may be punished as contempt of the issuing or denying judge.

"(d) Within a reasonable time but not later than ninety days after the filing of an application for an order of approval under section 2518(7)(b) which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, an inventory which shall include notice of—

"(1) the fact of the entry of the order or the application;

"(2) the date of the entry and the period of authorized, approved or disapproved interception, or the denial of the application; and

"(3) the fact that during the period wire or oral communications were or were not intercepted.

The judge, upon the filing of a motion, may in his discretion make available to such person or his counsel for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice. On an ex parte showing of good cause to a judge of competent jurisdiction the serving of the inventory required by this subsection may be postponed.

"(9) The contents of any intercepted wire or oral communication or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a Federal or State court unless each

party, not less than ten days before the trial, hearing, or proceeding, has been furnished with a copy of the court order, and accompanying application, under which the interception was authorized or approved. This ten-day period may be waived by the judge if he finds that it was not possible to furnish the party with the above information ten days before the trial, hearing, or proceeding and that the party will be prejudiced by the delay in receiving such information.

"(10) (a) Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any intercepted wire or oral communication, or evidence derived therefrom, on the grounds that—

"(i) the communication was unlawfully intercepted;

"(ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or

"(iii) the interception was not made in conformity with the order of authorization or approval.

Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. If the motion is granted, the contents of the intercepted wire or oral communication, or evidence derived therefrom, shall be treated as having been obtained in violation of this chapter. The judge, upon the filing of such motion by the aggrieved person, may in his discretion make available to the ag-

grieved person or his counsel for inspection such portions of the intercepted communication or evidence derived therefrom as the judge determines to be in the interests of justice.

"(b) In addition to any other right to appeal, the United States shall have the right to appeal from an order granting a motion to suppress made under paragraph (a) of this subsection, or the denial of an application for an order of approval if the United States attorney shall certify to the judge or other official granting such motion or denying such application that the appeal is not taken for purposes of delay. Such appeal shall be taken within thirty days after the date the order was entered and shall be diligently prosecuted.

Reports concerning intercepted wire or oral communications

"(1) Within thirty days after the expiration of an order (or each extension thereof) entered under section 2518, or the denial of an order approving an interception, the issuing or denying judge shall report to the Administrative Office of the United States Courts—

"(a) the fact that an order or extension was applied for;

"(b) the kind of order or extension applied for;

"(c) the fact that the order or extension was granted as applied for, was modified, or was denied;

"(d) the period of interceptions authorized by the order, and the number and duration of any extensions of the order;

"(e) the offense specified in the order or application, or extension of an order;

"(f) the identity of the applying investigative or law enforcement officer and agency making the application and the person authorizing the application; and

"(g) the nature of the facilities from which or the place where communications were to be intercepted.

"(2) In January of each year the Attorney General, an Assistant Attorney General specially designated by the Attorney General, or the principal prosecuting attorney of a State, or the principal prosecuting attorney for any political subdivision of a State, shall report to the Administrative Office of the United States Courts—

"(a) the information required by paragraphs (a) through (g) of subsection (1) of this section with respect to each application for an order or extension made during the preceding calendar year;

"(b) a general description of the interceptions made under such order or extension, including (i) the approximate nature and frequency of incriminating communications intercepted, (ii) the approximate nature and fequency of other communications intercepted, (iii) the approximate number of persons whose communications were intercepted, and (iv) the approximate nature, amount, and cost of the manpower and other resources used in the interceptions;

"(c) the number of arrests resulting from interceptions made under such order or extension, and the offenses for which arrests were made;

"(d) the number of trials resulting from such interceptions;

"(e) the number of motions to suppress made with respect to such interceptions, and the number granted or denied;

"(f) the number of convictions resulting from such interceptions and the offenses for which the convictions were obtained and a general assessment of the importance of the interceptions; and

"(g) the information required by paragraphs (b) through (f) of this subsection with respect to orders or extensions obtained in a preceding calendar year.

"(3) In April of each year the Director of the Administrative Office of the United States Courts shall transmit to the Congress a full and complete report concerning the number of applications for orders authorizing or approving the interception of wire or oral communications and extensions granted or denied during the preceding calendar year. Such report shall include a summary and analysis of the data required to be filed with the Administrative Office by subsections (1) and (2) of this section. The Director of the Administrative Office of the United States Courts is authorized to issue binding regulations dealing with the content and form of the reports required to be filed by subsections (1) and (2) of this section.

Recovery of civil damages authorized

"Any person whose wire or oral communication is intercepted, disclosed, or used in violation of this chapter shall (1) have a civil cause of action against any person who intercepts, discloses, or uses, or procures any other person to intercept, disclose, or use such communications, and (2) be entitled to recover from any such person–

"(a) actual damages but not less than liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is higher;

"(b) punitive damages; and

"(c) a reasonable attorney's fee and other litigation costs reasonably incurred.

A good faith reliance on a court order or on the provisions of section 2518(7) of this chapter shall constitute a complete defense to any civil or criminal action brought under this chapter."

Sec. 803. Section 605 of the Communications Act of 1934 (48 Stat. 1103; 47 U.S.C. 605) is amended to read as follows:

Unauthorized publication of communications

"Sec. 605. Except as authorized by chapter 119, title 18, United States Code, no person receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof, except through authorized channels of transmission or reception, (1) to any person other than the addressee, his

agent, or attorney, (2) to a person employed or authorized to forward such communication to its destination, (3) to proper accounting or distributing officers or the various communicating centers over which the communication may be passed, (4) to the master of a ship under whom he is serving, (5) in response to a subpena issued by a court of competent jurisdiction, or (6) on demand of other lawful authority. No person not authorized by the sender shall intercept any radio communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person. No person not being entitled thereto shall receive or assist in receiving any interstate or foreign communication by radio and use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto. No person having received any intercepted radio communication or having become acquainted with the contents, substance, purport, effect, or meaning of such communication (or any part thereof) knowing that such communication was intercepted, shall divulge or publish the existence, contents, substance, purport, effect, or meaning of such communication (or any part thereof) or use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto. This section shall not apply to the receiving, divulging, publishing, or utilizing the contents of any radio communication which is broadcast or transmitted by amateurs or others for the use of the general public, or which relates to ships in distress."

EPILOGUE

Despite the increasing number of antibugging devices and sophisticated electronic equipment on the market today, the single most effective antibugging device is a closed mouth!

The martini confidence can reveal more than a week's wiretap. Professional men – doctors, lawyers, real-estate men – who have much to lose often are the worst offenders in loose talk, boasting, or confiding secrets over drinks.

Yachtsmen and boat owners in a relaxed vacation mood may be easy targets for bugging. Any small bug would work in the slip itself in a marina, and a long-range transmitter, utilizing the boat's own power, can transmit an infinite amount of valuable information. When in a relaxed mood, far from land, and with a drink in his hand the unwary boat owner may discuss many taboo subjects.

An expert in the field of debugging says, "Prevention is the best debugging device – just learn to keep your mouth shut. And teach your wife and kids and employees to do the same."

Another expert in bugging and debugging says, "Most bugging jobs are ordered by a parent or spouse. I do these jobs for as little as $50 to $150, so anybody can afford it, I guess."

A safe rule to follow is that Big Brother or somebody probably *is* listening.

THE END

APPENDIX:

Radio Bands and Their Uses

10-30 KHz Very low frequency (VLF)	Point to point communication, long distance.
30-300 KHz Low frequency (LF)	Marine, submarine, navigational aids.
300-3000 KHz Medium frequency (MF)	Broadcasting AM, marine.
3-30 MHz High frequency (HF)	All types of communications, including amateur allotments.
30-300 MHz Very high frequency (VHF)	Radio FM, television, radar, air navigation, short wave.
300-3000 MHz Ultra high frequency (UHF)	Short distance point to point communication, radar, microwave relay.
3000-30,000 MHz Super high frequency (SHF)	Radar, microwave relay, navigation, experimental.
30-300 GHz Extremely high frequency (EHF)	Experimental, including CATV relays.

The majority of bugs are operated in the 30-50 and 70-90 MHz frequencies. They are not likely to be found in the 108-136, since this is the air-traffic control band and interference could cause serious repercussions.

The size of the antenna required is a limiting factor in the selection of an operating frequency. The lower the frequency the longer the antenna needed, since the antenna length is a function of the wave length. For example, a transmitter on the LF band would require a half-wave antenna length of at least 500 meters. One on the VHF band at least 0.5 meter. At the top of the UHF band, the antenna need be only 5 centimeters.

GLOSSARY

Absorption wavemeter. *A tunable instrument to detect radiation by means of a resonance. Adaptable to searching for bug-transmitters.*

Binaural. *An installation utilizing two microphones in order to give a stereophonic effect and greater intelligibility.*

Bridge. *A direct tap by connecting to, or "bridging," both wires in the pair.*

Bug. *A hidden microphone in eavesdropping argot. The majority of bugs are hooked to radio transmitters, although some may use wires as a pathway to the monitoring post.*

Bumper-Beeper. *An oscillator or signal generator affixed to a vehicle to serve as a beacon or homing device for tailing.*

Central office. *The local telephone company exchange.*

Common battery system. *The system whereby all telephones in an area served by the central office are powered by direct current cells in the central office.*

Contact mike. *A microphone that picks up sounds by amplifying the vibrations transmitted by a solid surface such as wall or door.*

Crosstalk. *The faint sound of another conversation sometimes picked up on a telephone. Caused by inductive pickup from another subscriber's pair in the same cable. Atmospheric conditions affect crosstalk.*

Crystal-controlled. *A transmitter and/or receiver whose frequency is fixed by a crystal as opposed to those with variable tuners. The advantage of crystals is that they are not susceptible to drift.*

Drop wire. *The insulated wires carrying the subscriber's phone pair from his building to a pole terminal box. The insulation usually is synthetic rubber or plastic. The drop wire may be routed to the box via a run-out on aerial cable to avoid trees or other obstructions.*

Grid-dip meter. *A variation of an absorption wavemeter that has itis own oscillator. By switching the oscillator off, the grid-dip meter can be used as a bug detector.*

Harmonics. *Multiple frequencies of a basic frequency. Their presence suggests a clandestine emission.*

Hot mike. *See mike-tel.*

IE. *Common term for industrial espionage.*

Impedance. *The resistance of a circuit to the flow of alternating current. Measured in ohms, it is calculated by dividing the voltage by the amperage. Thus circuits with low current drain, such as are desirable in most eavesdropping applications, tend to be of high impedance.*

Induction coil. *A coil with hundreds or thousands of turns of insulated wire wound on a cylinder. Some coils have an iron core. In eavesdropping, can be used to pick up sound without making a direct connection.*

Jammer. *A device that generates radiations that produce "hash" noises in hidden mikes, so that conversations are unintelligible to the listener. Also called "defeaters."*

Jumper wire. *A short pair of wires used to connect the subscribers phone pair to a leased line.*

Mail cover. *Interception of mail by the Post Office for a government agency.*

Mike-tel. *Contraction for microphone telephone, in which the phone instrument mike is converted to act as a mike pickup for room sounds as well as telephone conversations. Also called a hot mike.*

Mounting cord. *The insulated wires from the telephone instrument to a room connecting block.*

Multiple appearance. *An extra appearance of a subscriber's pair in a pole box other than the pole box to which his drop wire is connected. Created to allow for party lines, the multiple appearance permits tapping in relative security.*

Oscillator. *A device that generates radio waves. An RF oscillator generates a radio frequency carrier.*

Pair. *Telco parlance for the two wires constituting a subscriber's circuit.*

Parabolic mike. *A saucer-shaped device that gathers and focuses sound waves from a distance, then amplifies them.*

Parasitic devices. *A type of eavesdropping device that pirates its operating power from an established source such as telco battery and house current. Thus it requires no battery of its own.*

Pole box. *The pole terminal box for telephone pairs fastened to the telephone pole. Ordinarily accommodates 26 subscriber pairs, in two columns of 12 each.*

S-meter. *A field strength meter. Used in aligning receiver circuits, it is adaptable to the detection of bug-transmitters. Also used by tailers in conjunction with a Bumper-Beeper.*

Scrambler. *A pair of devices that scramble the voice signal on one end of a communication medium and descramble it on the receiving end. Most invert the voice signal. Thus anyone intercepting along the medium will hear only garbled voices.*

Spike mike. *Similar to the contact mike, but has a metal spike that is driven into the solid material, e.g. wall, duct, to pick up the voice vibrations.*

Sweep. *An electronic search for hidden bug-transmitters. Coupled with physical search to verify that premises are "clean."*

Tap. *The interception of communications by wire, as opposed to by wireless. A wiretap is generally a telephone tap.*

Telco. *Convenient contraction for one of the telephone operating companies.*

Western Electric. *The equipment manufacturer for the Bell System. Lenkurt Electric is the equipment manufacturer for the General Telephone System, the nation's second largest combine of operating companies.*

Wired mike. *An installation in which the microphone is connected to the monitoring post by means of wires.*

Wired wireless. *A term for an installation in which the premises' electric power line is used to carry the voice signal.*

Wireless bug. *A mike coupled to a radio transmitter.*

Working appearance. *The lugs in a pole terminal box to which the subscriber's pair is attached. The drop wire from the premises is fastened to the lugs. From the lugs, the pair joins the serial cable containing other subscribers' pairs.*